Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.1313

(07/2004)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE NOUVELLE GÉNÉRATION

Aspects relatifs au protocole Internet – Transport

Architectures de service et de réseau du réseau privé virtuel de couche 1

Recommandation UIT-T Y.1313

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE NOUVELLE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
RÉSEAUX DE LA PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de nouvelle génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.1313

Architectures de service et de réseau du réseau privé virtuel de couche 1

Résumé

La présente Recommandation spécifie les fonctions et les architectures permettant la prise en charge des services VPN de couche 1 décrits dans la Rec. UIT-T Y.1312 et contient également des exemples d'architectures détaillés.

Source

La Recommandation UIT-T Y.1313 a été approuvée le 22 juillet 2004 par la Commission d'études 13 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

Mots clés

Architecture, couche 1, fonction, réseau privé virtuel, VPN, VPN de couche 1.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T Y.1313

Architectures de service et de réseau du réseau privé virtuel de couche 1

1 Domaine d'application

La présente Recommandation décrit les fonctions et les architectures nécessaires à la prise en charge des services VPN de couche 1 définis dans la Rec. UIT-T Y.1312. Elle contient certains exemples d'architectures associées à l'utilisation de ressources du Plan C et du Plan U spécialisées ou communes. Pour les architectures, des exemples de réseaux sont donnés dans lesquels les fonctions sont décentralisées ou centralisées.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

2.1 Références normatives

[UIT-T G.805] Recommandation UIT-T G.805 (2000), *Architecture fonctionnelle générale des réseaux de transport*.

[UIT-T G.807] Recommandation UIT-T G.807/Y.1302 (2001), *Prescriptions relatives aux réseaux de transport à commutation automatique*.

[UIT-T G.7713.1] Recommandation UIT-T G.7713.1/Y.1704.1 (2003), *Gestion répartie des appels et des connexions: basée sur l'interface réseau-réseau privée (PNNI)*.

[UIT-T G.7713.2] Recommandation UIT-T G.7713.2/Y.1704.2 (2003), *Gestion répartie des appels et des connexions: Mécanisme de signalisation DCM utilisant l'élément RSVP-TE de la commutation multiprotocolaire généralisée par étiquettes (GMPLS)*.

[UIT-T G.7713.3] Recommandation UIT-T G.7713.3/Y.1704.3 (2003), *Gestion répartie des appels et des connexions: Mécanisme de signalisation utilisant le protocole de distribution par étiquetage à acheminement par contraintes (CR-LDP) de la commutation multiprotocolaire généralisée par étiquettes (GMPLS)*.

[UIT-T G.7714.1] Recommandation UIT-T G.7714.1/Y.1705.1 (2003), *Protocole d'exploration automatique dans les réseaux à hiérarchie numérique synchrone et les réseaux de transport optiques*.

[UIT-T G.8080] Recommandation UIT-T G.8080/Y.1304 (2001), *Architecture du réseau optique à commutation automatique (ASON)*.

[UIT-T Y.1311] Recommandation UIT-T Y.1311 (2002), *Réseaux virtuels privés fournis par le réseau – Architecture générique et prescriptions de service*.

[UIT-T Y.1312] Recommandation UIT-T Y.1312 (2003), *Prescriptions génériques et éléments architecturaux pour les réseaux privés virtuels de couche 1*.

[IETF RFC 1771] IETF RFC 1771 (1995), *A Border Gateway Protocol 4 (BGP-4)*.

[IETF RFC 2328] IETF RFC 2328 (1998), *OSPF version 2*.

[IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.

[IETF RFC 3472] IETF RFC 3472 (2003), *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions*.

[IETF RFC 3473] IETF RFC 3473 (2003), *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*.

[OIF UNI 1.0] OIF Implementation Agreement OIF-UNI01.0 (2001), *User Network Interface (UNI) 1.0 Signaling Specification*.

[OIF Signaling E-NNI 1.0] OIF Implementation Agreement OIF-E-NNI-Sig-01.0 (2004), *Intra-Carrier E-NNI Signaling Specification*.

2.2 Références informatives

[IETF RFC 3474] IETF RFC 3474 (2003), *Documentation of IANA assignments for Generalized MultiProtocol Label Switching (GMPLS) Resource Reservation Protocol – Traffic Engineering (RSVP-TE) Usage and Extensions for Automatically Switched Optical Network (ASON)*.

[IETF RFC 3475] IETF RFC 3475 (2003), *Documentation of IANA assignments for Constraint-Based LSP setup using LDP (CR-LDP) Extensions for Automatic Switched Optical Network (ASON)*.

[IETF RFC 3476] IETF RFC 3476 (2003), *Documentation of IANA Assignments for Label Distribution Protocol (LDP), Resource ReSerVation Protocol (RSVP), and Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) Extensions for Optical UNI Signaling*.

3 Définitions

3.1 La présente Recommandation fait usage des termes suivants définis dans les Recommandations UIT-T suivantes:

a) **VPN L1 (VPN de couche 1)**: voir la Rec. UIT-T Y.1312.

b) **extrémité CE**: voir la Rec. UIT-T Y.1312.

c) **extrémité PE**: voir la Rec. UIT-T Y.1312.

d) **P**: voir la Rec. UIT-T Y.1312.

e) **client**: voir la Rec. UIT-T Y.1312.

f) **plan U partagé**: voir la Rec. UIT-T Y.1312.

g) **plan U exclusif**: voir la Rec. UIT-T Y.1312.

h) **plan C partagé**: voir la Rec. UIT-T Y.1312.

i) **plan C exclusif**: voir la Rec. UIT-T Y.1312.

j) **connexion**: voir la Rec. UIT-T Y.1312.

k) **CP (point de connexion)**: voir la Rec. UIT-T G.805.

l) **liaison**: voir les Recommandations UIT-T G.805 et Y.1312.

m) **connexion de liaison**: voir la Rec. UIT-T G.805.

n) **sous-réseau**: voir la Rec. UIT-T G.805.

o) **chemin**: voir la Rec. UIT-T G.805.

p) **point de sous-réseau (SNP)**: voir la Rec. UIT-T G.8080/Y.1304.

q) **pool de points de sous-réseau (SNPP)**: voir la Rec. UIT-T G.8080/Y.1304.

r) **connexion de liaison SNP**: voir la Rec. UIT-T G.8080/Y.1304.

s) **liaison SNPP**: voir la Rec. UIT-T G.8080/Y.1304.

3.2 La présente Recommandation définit les termes suivants:

3.2.1 contrôleur centralisé du fournisseur (PCC, *provider centralized controller*): entité centralisée qui exécute certaines fonctions VPN L1 pour le réseau du fournisseur.

3.2.2 contrôleur centralisé du client (CCC, *customer centralized controller*): entité centralisée qui exécute certaines fonctions VPN L1 pour le réseau du client.

3.2.3 entité fournisseur: entité qui exécute certaines fonctions VPN L1 pour le réseau du fournisseur. L'entité fournisseur peut être l'extrémité PE/P ou le contrôleur PCC, selon l'implémentation des fonctions.

3.2.4 entité client: entité qui exécute certaines fonctions VPN L1 pour le réseau client. L'entité client peut être l'extrémité CE ou le contrôleur CCC, selon l'implémentation des fonctions.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AAA authentification, autorisation et comptabilité (*authentication, authorization and accounting*)

BGP protocole de passerelle frontière (*border gateway protocol*)

CCC contrôleur centralisé du client (*customer centralized controller*)

CE extrémité client (*customer edge*)

CNM gestion de réseau client (*customer network management*)

COPS service commun de politique ouverte (*common open policy service*)

CORBA architecture de courtier commun de requête d'objets (*common object request broker architecture*)

CP point de connexion (*connection point*)

CUG groupe fermé d'utilisateurs (*closed user group*)

E-NNI interface externe réseau-réseau (*external network-to-network interface*)

EPL ligne privée Ethernet (*Ethernet private line*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

GMPLS commutation multiprotocolaire généralisée par étiquettes (*generalized multi-protocol label switching*)

I-NNI interface interne réseau-réseau (*internal network-to-network interface*)

LRM gestionnaire de ressources de liaison (*link resource manager*)

NNI interface réseau-réseau (*network-to-network interface*)

OAM gestion, exploitation et maintenance (*operation, administration and maintenance*)

OSPF plus court chemin ouvert en premier (*open shortest path first*)

OTN réseau de transport optique (*optical transport network*)

P fournisseur (*provider*)

PCC contrôleur centralisé du fournisseur (*provider centralized controller*)

PDP point de décision de politique (*policy decision point*)

PE extrémité fournisseur (*provider edge*)

PEP point d'application des politiques (*policy enforcement point*)

RCD réseau de communication de données

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SNP point de sous-réseau (*subnetwork point*)

SNPP pool de points de sous-réseau (*subnetwork point pool*)

SPC connexion permanente reconfigurable (*soft permanent connection*)

TCA alerte de dépassement de seuil (*threshold crossing alert*)

TL1 langage de transaction 1 (*transaction language 1*)

TMF TeleManagement Forum

UNI interface utilisateur-réseau (*user network interface*)

VPN réseau privé virtuel (*virtual private network*)

XML langage de balisage extensible (*extensible markup language*)

5 Classement des fonctions

Pour pouvoir prendre en charge les fonctions de service, le réseau assurant le service VPN L1 doit exécuter les fonctions suivantes décrites dans la Rec. UIT-T Y.1312, certaines de ces fonctions pouvant être optionnelles.

Figure 5-1/Y.1313 – Modèle de référence de VPN de couche 1 avec entités fonctionnelles

Les entités fonctionnelles décrites à la Figure 5-1 peuvent être en outre catégorisées comme suit, parallèlement à d'autres fonctions.

1) *Tenue à jour de la liste des membres*

Echange et tenue à jour des informations relatives aux membres, incluant les fonctions suivantes:

- distribution des informations relatives aux membres (entre le client et le réseau);
- distribution des informations relatives à la disponibilité des membres (entre le client et le réseau);
- tenue à jour de la liste des membres (uniquement dans le réseau);
- mappage CE-VPN (uniquement dans le réseau).

2) *Tenue à jour des informations d'acheminement et calcul de trajet*

A) *Tenue à jour des informations d'acheminement*

Cela concerne l'échange et la tenue à jour des informations impliquant les informations relatives à la topologie (à la fois pour le réseau et pour le client). En particulier, on distingue trois types d'informations de tenue à jour des informations d'acheminement, à savoir: l'information relative au domaine d'acheminement du client, l'information relative à la topologie du réseau et l'information de connectivité. L'information relative au domaine d'acheminement du client peut être tenue à jour dans le réseau et utilisée pour l'optimisation des trajets ou peut être transférée de manière transparente entre les entités clients. L'information sur la topologie du réseau et une partie de cette information par réseau VPN individuel peuvent être transférées au client. L'information sur la topologie inclut les informations sur la façon dont les liaisons sont interconnectées ainsi que celles qui concernent l'utilisation des ressources. L'information de connectivité porte sur la façon dont les entités CE sont connectées les unes aux autres et peut inclure des informations sur le trajet sur lequel la connexion est acheminée. Les entités fonctionnelles classées comme concernant la tenue à jour des informations d'acheminement incluent les fonctions permettant de tenir à jour les trois types d'informations précités dans le réseau, ainsi que les fonctions permettant de transférer ces types d'informations entre le client et le réseau.

La tenue à jour des informations d'acheminement fait intervenir les fonctions suivantes:

– la participation du réseau dans le domaine d'acheminement du client (entre le client et le réseau);
– le transfert des informations sur les ressources par réseau VPN individuel (entre le client et le réseau);
– le transfert des informations de connectivité par réseau VPN individuel (entre le client et le réseau);
– la tenue à jour des informations dans le domaine d'acheminement du client (uniquement dans le réseau);
– la tenue à jour des informations sur la topologie du réseau (uniquement dans le réseau);
– la tenue à jour des informations de connectivité (uniquement dans le réseau);
– le transfert transparent de l'information de commande entre des entités clients (entre le client et le réseau).

  A noter que le transfert transparent de l'information de commande entre des entités clients concerne en général le transfert de l'information d'acheminement, mais peut aussi être utilisé pour transférer d'autres informations.

B) *Calcul de trajet*

Le calcul de trajet est le mécanisme qui permet de sélectionner des liaisons en vue de la constitution d'une connexion, en utilisant l'information de topologie obtenue par les fonctions de tenue à jour des informations d'acheminement, ainsi que par l'utilisation de restrictions et/ou de préférences spécifiées dans les politiques. Après le calcul d'un trajet, une connexion est établie le long de ce trajet par des fonctions de commande de connexion.

Le calcul de trajet fait intervenir les fonctions suivantes:

– sélection de liaisons (uniquement dans le réseau);
– sélection explicite de liaisons (uniquement chez le client).

3) *Commande de connexion*

Cette fonctionnalité est liée à l'échange d'informations et à la configuration des connexions faisant intervenir l'établissement/la suppression/la demande de modification d'une connexion ou la réponse et fait intervenir les fonctions suivantes:

– commande dynamique d'une connexion de couche 1 (entre le client et le réseau);
– le traitement des connexions (uniquement dans le réseau);
– notification du rejet d'une connexion (entre le client et le réseau).

4) *Gestion*

La gestion est liée au processus de décision ainsi qu'à la consignation et au traitement des erreurs concernant les fonctions précitées, et fait intervenir les fonctions suivantes:

A) *Authentification, autorisation et comptabilité (AAA, authentication, authorization, accounting)*

– Authentification (entre le client et le réseau).
– Autorisation (uniquement dans le réseau).
– Comptabilité (uniquement dans le réseau).

B) *Politiques*

Les politiques servent à préciser comment réagir à des événements particuliers: le calcul de trajet, d'anomalie ou autre. Ces politiques peuvent donc constituer une entrée tant pour le calcul de routage que pour les opérations d'exploitation et de maintenance ou le traitement des pannes. Les politiques en matière de calcul de trajet permettent de définir les paramètres décrivant le type de connexion préféré (par exemple en faisant une pondération à chaque liaison), tandis que les politiques relatives au traitement des anomalies préciseront les réactions, comportement visant à protéger et à rétablir telle ou telle connexion. Des politiques sont également appliquées au contrôle d'admission des demandes de connexion, y compris les restrictions de connectivité entre différents réseaux VPN ou à l'intérieur du même réseau VPN, ainsi que la confirmation de la classe de service L1 demandée au regard du contrat de service.

Les politiques font intervenir les fonctions suivantes:

– la politique individuelle par extrémité CE et sa gestion (entre le client et le réseau);
– la politique individuelle par réseau VPN (uniquement dans le réseau);
– les restrictions de connectivité (uniquement dans le réseau);
– sélection de la classe de service L1 (uniquement chez le client);
– le mappage de la classe de service avec les mécanismes de survivabilité (uniquement dans le réseau).

C) *OAM et traitement des anomalies*

L'OAM et le traitement des anomalies peuvent être fondés sur des politiques. Par exemple, la protection et le comportement de rétablissement peuvent différer en fonction des politiques pour chaque connexion et/ou chaque réseau VPN.

L'OAM et le traitement des anomalies font intervenir les fonctions suivantes:

– transfert des informations de performance (entre le client et le réseau);
– le transfert des informations relatives aux anomalies (entre le client et le réseau);
– la supervision de la performance (uniquement dans le réseau);
– gestion des anomalies (uniquement dans le réseau).

D) *Vérification de la configuration VPN de couche 1*

Il devrait exister certains mécanismes permettant de s'assurer que la configuration a correctement été établie. Les mécanismes associés à cette fonction appellent un complément d'étude.

5) *Autres*

Nous donnons ci-après une liste des fonctions spécifiques aux réseaux VPN autres que de couche 1, requises pour le réseau VPN de couche 1 conformément aux fonctions précitées:

– acheminement dans le plan commande (par exemple acheminement RCD);
– exploration et tenue à jour des informations relatives aux ressources des liaisons (par exemple LRM).

A noter que les fonctions détaillées peuvent différer selon les scénarios d'activité. Ce point appelle un complément d'étude. Il convient également de noter que ces entités fonctionnelles utilisent uniquement seulement les fonctions qu'elles peuvent exécuter et n'impliquent pas une implémentation particulière. De plus, plusieurs entités fonctionnelles peuvent être implémentées par le même mécanisme. Par exemple, les fonctionnalités "commande de connexion" et "tenue à jour des informations d'acheminement" ou "transfert des informations sur les anomalies" peuvent être implémentées par le même mécanisme lorsqu'une information en retour émanant de la commande de connexion peut être utilisée pour la mise à jour de l'information concernant l'acheminement ou pour signaler une anomalie.

6 Scénarios de service, caractéristiques de service et fonctions requises

6.1 Description des fonctions avec les caractéristiques de service

Dans le § 5, on classe les fonctions en plusieurs modules. Parmi celles-ci, afin d'assurer des services VPN L1, il y a des fonctions essentielles telles que décrites dans la Rec. UIT-T Y.1312, à savoir la commande de connexion, la fonction AAA (sauf la comptabilité), les restrictions de connectivité des politiques, la tenue à jour des informations d'acheminement et le calcul de trajet dans le réseau, la tenue à jour des informations sur les membres dans le réseau, l'OAM et le traitement des anomalies dans le réseau. Ces fonctions permettent aux clients de lancer une demande de connexion entre extrémités CE à l'intérieur du même réseau VPN, au fournisseur de choisir un trajet pour une connexion et de gérer le réseau.

Si le client souhaite connaître la liste des extrémités CE à l'intérieur du même réseau VPN, il est nécessaire de pouvoir prendre en charge les fonctions relatives aux membres. Cette caractéristique de service est importante, en particulier lorsque les extrémités CE participent au réseau VPN de manière dynamique. Si le client souhaite recevoir un service différencié, des capacités permettant de spécifier des politiques par réseau VPN sont nécessaires. De même, si aux extrémités CE d'un même réseau VPN on souhaite avoir différents niveaux de service, la présence de capacités permettant de spécifier une politique par extrémités CE est requise. Dans le cas d'une seule administration, ce qui signifie que chaque extrémité CE du même réseau VPN relève de la même administration, il peut être nécessaire d'avoir une politique par réseau VPN et éventuellement une politique par extrémité CE. Dans le cas de plusieurs administrations, ce qui signifie que les limites CE du même réseau VPN appartiennent à des administrations différentes, il serait nécessaire de définir une politique commune sur l'ensemble du réseau VPN. Si le client souhaite recevoir des informations OAM ou sur les anomalies, afin de lui permettre de prendre une décision concernant la réaction à des dérangements, la présence de fonctions OAM et de traitement des anomalies est nécessaire entre le client et le réseau. Si le client souhaite connaître la topologie interne du réseau du fournisseur de sorte que le client puisse exercer un contrôle plus grand sur l'acheminement des connexions (par exemple, en cas d'ingénierie perfectionnée du trafic), il est nécessaire que le client dispose d'informations d'acheminement. Le client calcule le trajet associé à une nouvelle demande

de connexion. Ces caractéristiques de service sont des caractéristiques additionnelles à valeur ajoutée.

A noter qu'une politique par réseau VPN est une caractéristique essentielle pour le fournisseur, mais les clients ne doivent pas nécessairement l'utiliser. Dans ce contexte, une politique par réseau VPN est une caractéristique de service à valeur ajoutée du point de vue du client.

Tableau 6-1/Y.1313 – Fonctions avec caractéristiques de service

Fonctions		Caractéristiques de service
Tenue à jour des informations sur les membres		– Gestion dynamique des membres
Tenue à jour des informations d'acheminement et calcul de trajet		– Disposer d'une capacité de conception de réseau pour les clients (participation du client à l'ingénierie de trafic)
Commande de connexion		– Obligatoire
Gestion	AAA	– Obligatoire (sauf pour la comptabilité)
	Politiques	– La restriction de connectivité est obligatoire – Assurer des services différenciés, ainsi que différentes politiques par CE
	OAM et traitement des anomalies	– Offrir aux clients la possibilité de connaître ce qui se passe dans le réseau, ce qui peut permettre aux clients de prendre des décisions concernant la façon de réagir.

6.2 Exemples de scénarios de service et de fonctions requises

Sont décrits ici plusieurs scénarios de service possibles dont certains proviennent de la Rec. UIT-T Y.1312, ainsi que les caractéristiques de service souhaitées et les fonctions requises.

– *Distribution de contenu (par exemple réflexion)*

  Dans ce scénario, les clients exigent une forte capacité de retransmission du contenu, basée sur la nécessité. L'échelle de temps nécessaire pour demander/libérer des connexions est de l'ordre de quelques heures, ou reposer éventuellement sur une programmation quotidienne ou hebdomadaire. Le nombre d'extrémités CE devrait être relativement faible. Toutes les extrémités CE peuvent relever de la même administration (retransmission à l'intérieur de la même organisation), ou de différentes administrations (retransmission dans des organisations différentes). Les informations sur les membres tendent à être statiques (retransmission avec le même ensemble de limites CE, quotidien ou hebdomadaire). Les clients sont considérés comme étant moins impliqués dans la gestion du réseau optique.

  La possibilité d'offrir des connexions multipoint à point est une caractéristique exigée, et la conception de l'ensemble du réseau, en recourant à une ingénierie de trafic complexe pour des profils de trafic dynamique, n'est pas nécessaire.

  En plus des fonctions obligatoires permettant de prendre en charge les services VPN L1, on pourrait exiger la présence de fonctions OAM et de traitement des anomalies. Il peut être nécessaire pour les clients de disposer d'une politique par réseau VPN lorsque les extrémités CE relèvent d'une même administration, s'ils veulent bénéficier de services différenciés.

– *Vidéoconférence*

  Dans ce scénario, un groupe d'extrémités CE est formé, et l'information concernant la vidéoconférence est transférée parmi elles. Des connexions sont nécessaires uniquement pendant la tenue de la vidéoconférence. Les extrémités CE à l'intérieur du même groupe

peuvent relever de différentes administrations. Un groupe peut être formé de manière dynamique, signifiant une participation dynamique des extrémités CE, ainsi qu'une entité dynamique du groupe lui-même. Les clients sont considérés comme étant moins impliqués dans la gestion du réseau optique. Cette situation est analogue à un service public avec groupe fermé d'utilisateurs.

Dans ce scénario, il peut s'avérer difficile de définir une politique commune à l'ensemble du réseau VPN, en particulier si les extrémités CE relèvent de différentes administrations.

Outre les fonctions obligatoires permettant de prendre en charge les services VPN L1, il peut être nécessaire d'avoir les fonctions relatives aux membres. Les fonctions OAM et de traitement des anomalies peuvent aussi s'avérer nécessaires pour offrir une caractéristique de service additionnelle.

– *Opérateur de l'opérateur*

Dans ce scénario, un opérateur qui reçoit un service VPN L1 d'un autre opérateur assure ses propres services. Le nombre d'extrémités CE peut être relativement important. Le trafic peut varier dans un intervalle de temps relativement faible (par exemple, variation de trafic diurne et nocturne) ainsi que dans le long terme ce qui en général implique un certain type de topologie du réseau. Les clients devraient être relativement habitués à gérer le réseau par eux-mêmes.

La capacité à configurer une topologie de réseau pour les clients est exigée. De même, sont exigées des politiques élaborées par réseau VPN et éventuellement par extrémité CE afin de pouvoir bien gérer le réseau.

Contre les fonctions obligatoires permettant la prise en charge des services VPN L1, les fonctions qui pourraient être requises sont les fonctions OAM et la gestion des anomalies et les fonctions relatives à la politique. Des fonctions relatives aux membres pourraient être également requises. La présence de fonctions associées à l'acheminement avec un échange limité de topologies peut s'avérer souhaitable, en fonction des besoins du service.

– *Infrastructure multiservice*

Dans ce scénario, un département service d'un opérateur recevant le service VPN L1 de l'opérateur assure différents types de service de couche supérieure. Le trafic peut varier dans un intervalle de temps relativement faible (par exemple, diurne et nocturne) ainsi que dans le long terme, ce qui implique généralement un certain type de topologie du réseau. Les clients devraient être relativement habitués à gérer le réseau par eux-mêmes.

La capacité à configurer une topologie de réseau pour les clients est exigée. De même, sont exigées des politiques élaborées par réseau VPN et éventuellement par extrémité CE afin de pouvoir bien gérer le réseau.

Outre des fonctions obligatoires permettant la prise en charge des services VPN L1, les fonctions qui pourraient être requises sont les fonctions OAM et la gestion des anomalies ainsi que des fonctions relatives à la politique. Des fonctions relatives aux membres pourraient être également requises. Comparé au cas opérateur de l'opérateur, on s'attend à ce qu'il y ait échange d'informations plus détaillées sur la topologie entre le client et le réseau. Les clients peuvent calculer le trajet en utilisant l'information de topologie donnée par le fournisseur.

Tableau 6-2/Y.1313 – Mappage des scénarios de service avec les fonctions requises

	Conditions					Fonctions requises
	Nombre de CE	**Profil du trafic**	**Utilisation sophistiquée du réseau par les clients**	**Appartenance**	**Administration**	
Distribution de contenus	Faible	Tout ou rien	Moins probable	Statique	Unique/multiple (les CE peuvent relever de la même administration ou d'administrations différentes)	OAM et gestion des anomalies (politiques)
Vidéo-conférence	Faible-grand	Tout ou rien	Moins probable	Dynamique	Multiple (les CE relèvent d'administrations différentes)	(OAM et gestion des anomalies), tenue à jour des informations sur les membres
Opérateur de l'opérateur	Grand	Variation à court terme et à long terme	Probable	Statique	Unique (chaque CE relève de la même administration)	OAM et gestion des anomalies, politiques (tenue à jour des informations sur les membres) (tenue à jour des informations d'achemi-nement et calcul de trajet)
Infras-tructure multi-service	Grand	Variation à court terme et à long terme	Probable	Statique	Unique (le fournisseur et le client relèvent de la même administration)	OAM et gestion des anomalies, politiques (tenue à jour des informations sur les membres) (tenue à jour des informations d'achemi-nement et calcul de trajet)

7 Classement des architectures

Sur la base des implémentations fonctionnelles, les architectures sont classées en plusieurs catégories à savoir décentralisées, centralisées ou hybrides. Dans le cas d'une architecture hybride, certaines fonctions sont décentralisées tandis que d'autres sont centralisées.

Bien qu'il puisse y avoir une certaine relation entre l'architecture côté fournisseur du réseau et l'architecture côté client du réseau, ces deux architectures de réseau seront décrites de façon séparée aux § 7.1 et 7.2 ci-dessous.

Les fonctions nécessaires à la gestion sont examinées de manière distincte au § 7.3.

7.1 Architecture de réseau côté fournisseur

Dans l'architecture de réseau côté fournisseur, certaines fonctions font intervenir un échange d'informations avec les clients et d'autres font intervenir un échange d'informations ou des actions uniquement à l'intérieur du réseau du fournisseur.

1) Architecture décentralisée

Dans une architecture décentralisée, les fonctions de la tenue à jour des informations sur les membres, des informations d'acheminement et du calcul de trajet, ainsi que la commande de connexion sont décentralisées ainsi que certaines fonctions de gestion. Dans l'architecture décentralisée, l'extrémité PE est l'entité qui permet de communiquer avec l'entité client, qui est généralement l'extrémité CE.

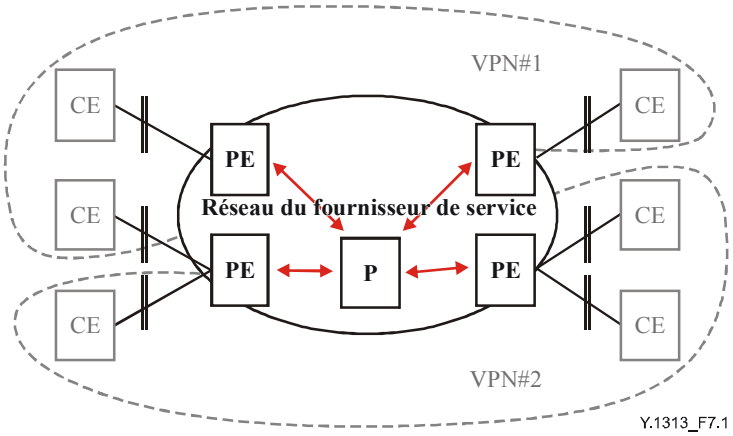

Figure 7-1/Y.1313 – Architecture décentralisée du réseau du fournisseur de service VPN L1

Sont données ci-après, en termes d'interaction et d'échange d'informations entre l'extrémité fournisseur (PE) et le fournisseur (P), certaines explications détaillées concernant l'architecture décentralisée du réseau du fournisseur ainsi que sur la façon dont sont exécutées les fonctions de tenue à jour des informations sur les membres, de tenue à jour des informations d'acheminement et de calcul de trajet ainsi que de commande de connexion décrites au § 5.

- *Tenue à jour des informations sur les membres*

L'extrémité PE contient les informations sur les membres tandis que l'entité fournisseur P ne contient pas nécessairement ces informations. Une extrémité PE peut directement communiquer avec les extrémités PE distantes, auprès desquelles elle peut obtenir toutes les informations sur les membres pour chaque réseau VPN. A noter que chaque extrémité PE n'a pas besoin d'obtenir les informations sur les membres d'un réseau VPN spécifique, lorsque l'extrémité PE n'est pas connectée aux entités clients relevant de ce réseau VPN. Ceci permet d'améliorer la modularité.

L'extrémité PE peut également communiquer avec les entités clients qui lui sont associées, afin d'obtenir les informations sur les membres du réseau VPN considéré, et de fournir des informations sur les membres au réseau VPN auquel ces entités clients appartiennent.

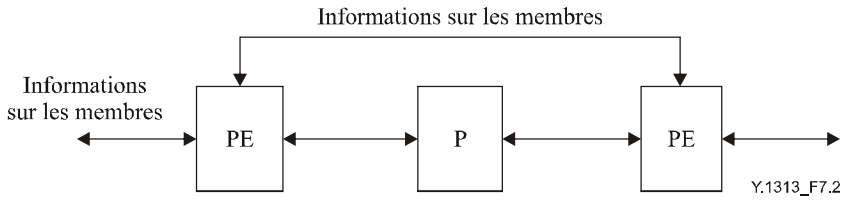

Figure 7-2/Y.1313 – Tenue à jour des informations sur les membres

- *Tenue à jour des informations d'acheminement et calcul de trajet*

A) *Tenue à jour des informations d'acheminement*

On distingue trois types d'informations qui font partie des informations d'acheminement, telles que décrites au § 5, à savoir: l'information d'acheminement du domaine client, l'information de topologie du réseau et l'information de connectivité. Ces types d'informations peuvent être acheminés par la même instance/le même mécanisme, ou par des instances ou des mécanismes différents.

a) *Information d'acheminement du domaine client*

Lorsque le réseau participe à un acheminement du domaine client, l'extrémité PE contient l'information d'acheminement du domaine client. Par ailleurs, l'entité P ne contient pas nécessairement d'informations d'acheminement du domaine client. Une extrémité PE peut directement communiquer avec des extrémités PE pour obtenir toute l'information d'acheminement du domaine client pour chaque réseau VPN. A noter qu'il n'est pas nécessaire pour une extrémité PE d'obtenir l'information d'acheminement du domaine client pour un réseau VPN particulier lorsque cette extrémité n'est pas connectée à des entités clients appartenant au réseau VPN considéré. Cela améliore la modularité.

Parallèlement, l'extrémité PE communique avec les entités clients associées à cette extrémité PE, afin d'obtenir l'information d'acheminement de ces domaines clients et de fournir l'information d'acheminement du domaine client du réseau VPN auquel sont rattachées ces entités clients.

Lorsqu'on souhaite obtenir un transfert transparent de l'information de commande entre entités clients, l'extrémité PE ou l'entité P ne contiennent pas nécessairement l'information d'acheminement du domaine client permettant à cette information de circuler de manière transparente entre entités clients.

b) *Information concernant la topologie du réseau*

L'extrémité PE et l'entité P contiennent toutes deux des informations concernant la topologie du réseau. L'extrémité PE et l'entité P communiquent avec les extrémités PE et les entités P connectées.

Parallèlement, l'extrémité PE peut communiquer avec les entités clients qui lui sont associées, afin de fournir de l'information sur la topologie du fournisseur de réseau. A noter que cela s'applique en général au cas d'un Plan U exclusif. L'information transférée vers les entités clients est limitée à la topologie particulière du réseau VPN auquel ces entités clients appartiennent. De même, l'information peut être transférée aux entités clients sous forme résumée (par exemple, en ne donnant pas la topologie détaillée).

c) *Information de connectivité*

L'extrémité PE contient l'information de connectivité, tandis que l'entité P ne la contient pas nécessairement. Une extrémité PE peut directement communiquer avec des extrémités PE distantes, auprès desquelles l'extrémité PE peut obtenir toute l'information de connectivité pour chaque réseau VPN. A noter qu'il n'est pas nécessaire pour une extrémité PE d'obtenir l'information de connectivité d'un réseau VPN spécifique, si cette extrémité n'est pas connectée aux entités clients appartenant à ce réseau. Cela améliore la modularité.

L'extrémité PE peut également communiquer avec les entités clients associées à cette extrémité, afin d'obtenir l'information de connectivité du réseau VPN considéré, et de fournir l'information de connectivité du réseau VPN auquel ces entités clients appartiennent.

B) *Calcul de trajet*

Un trajet peut être calculé par l'extrémité client (CE) et spécifié, par exemple, dans une demande de commande de connexion. Ou bien, un trajet peut être calculé par l'extrémité PE ou par l'extrémité PE et l'entité P.

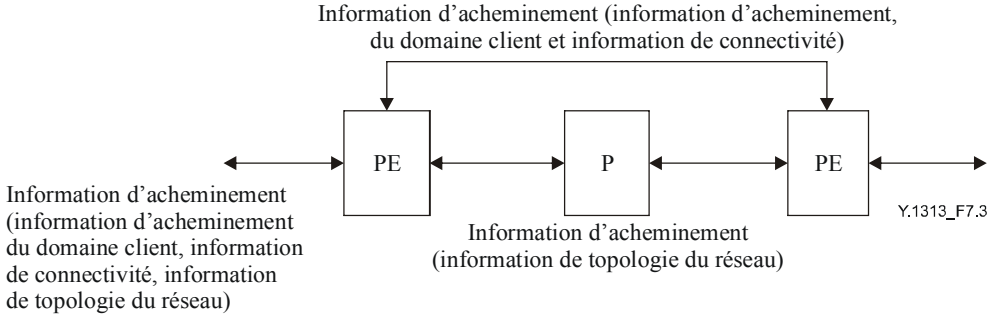

Figure 7-3/Y.1313 – Tenue à jour des informations d'acheminement et calcul de trajet

• *Commande de connexion*

L'extrémité PE et l'entité P contiennent des informations relatives à la commande de connexion et communiquent avec les extrémités PE et les entités P connectées. Il peut également y avoir échange direct d'informations relatives à la commande de connexion entre extrémités PE, par exemple, la commande de connexion propre au réseau VPN.

Parallèlement, l'extrémité PE communique avec les entités clients qui lui sont associées, afin de recevoir les demandes de connexion émanant de ces entités clients et d'envoyer des demandes de connexion aux entités clients situées à l'autre extrémité si besoin est.

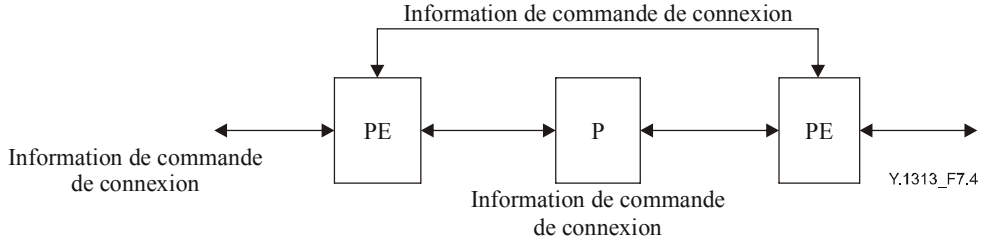

Figure 7-4/Y.1313 – Commande de connexion

A noter que les mécanismes ou les protocoles permettant d'échanger l'information à l'intérieur du réseau du fournisseur (entre extrémités PE, entre une extrémité PE et une entité P, entre entités P) et entre le réseau du fournisseur et le réseau du client (entre une extrémité PE et une entité client) peuvent être différents pour la tenue à jour des informations sur les membres, la tenue à jour de l'information d'acheminement et la commande de connexion.

2) Architecture centralisée

Dans le cas d'une architecture centralisée, les fonctions de tenue à jour des informations sur les membres, de tenue à jour de l'information d'acheminement et de calcul de trajet ainsi que la commande de connexion sont centralisées ainsi que certaines autres fonctions. L'entité centralisée peut être appelée contrôleur centralisé du fournisseur (PCC, *provider centralized controller*). Dans une architecture centralisée, le contrôleur PCC est l'entité qui permet de communiquer avec l'entité client, qui est généralement le contrôleur centralisé du client (CCC, *centralized customer controller*).

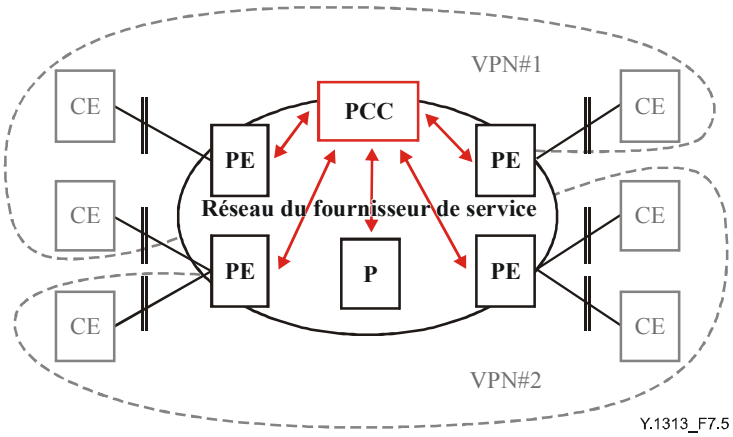

Figure 7-5/Y.1313 – Architecture centralisée de réseau du fournisseur de service VPN L1

Une explication plus détaillée de l'architecture centralisée du réseau du fournisseur est donnée ci-après, ainsi que la manière dont s'effectue la tenue à jour des informations sur les membres, la tenue à jour de l'information d'acheminement et le calcul de trajet et la commande de connexion, en termes d'interaction et d'échange d'informations, parmi les extrémités PE, l'entité P et le contrôleur PCC.

- *Tenue à jour des informations sur les membres*

Le contrôleur PCC contient les informations sur les membres, tandis que l'extrémité PE et l'entité P ne les contiennent pas nécessairement. Le contrôleur PCC peut communiquer avec les entités clients afin d'obtenir les informations sur les membres et, aussi, de transférer ces informations.

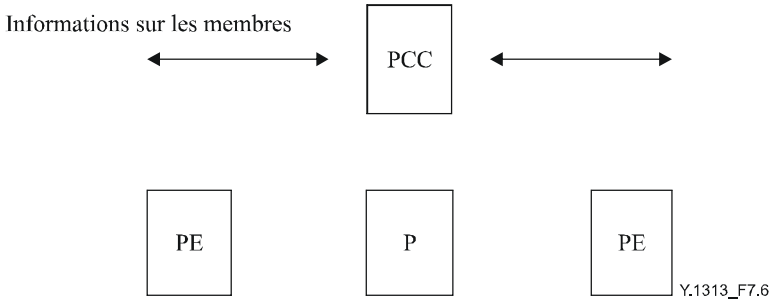

Figure 7-6/Y.1313 – Tenue à jour des informations sur les membres

- *Tenue à jour de l'information d'acheminement et calcul de trajet*

A) *Tenue à jour de l'information d'acheminement*

On distingue trois types d'informations qui relèvent de l'information d'acheminement, telle que décrite au § 5, à savoir: l'information du domaine client, l'information de topologie du réseau et l'information de connectivité.

a) *Information d'acheminement du domaine client*

Lorsque le réseau participe à l'acheminement du domaine client, le contrôleur PCC contient l'information d'acheminement du domaine client, mais il n'est pas nécessaire que l'extrémité PE et l'entité P contiennent l'information d'acheminement du domaine client.

Lorsqu'on souhaite obtenir un transfert transparent de l'information de commande entre les entités clients, il n'est pas nécessaire que le contrôleur PCC contienne l'information d'acheminement du domaine client. Le contrôleur PCC transfert simplement l'information qu'il reçoit d'une entité particulière à une ou plusieurs autres.

b) *Information de topologie du réseau*

Le contrôleur PCC, l'extrémité PE et l'entité P contiennent l'information de topologie du réseau. Le contrôleur PCC communique avec des extrémités PE et/ou des entités P, et obtient toute l'information de topologie du réseau. L'extrémité PE et l'entité P contiennent l'information de topologie locale, mais pas nécessairement l'information de topologie de tout le réseau. Parallèlement, le contrôleur PCC peut communiquer avec des entités clients afin de fournir l'information de topologie du réseau du fournisseur. A noter que cela s'applique en général au cas du Plan U exclusif. L'information transférée vers les entités clients est limitée à la topologie spéciale du réseau VPN auquel appartiennent ces entités clients. De même, l'information peut être transférée vers les entités clients sous forme résumée (par exemple, en ne donnant pas la topologie détaillée).

c) *Information de connectivité*

Le contrôleur PCC contient l'information de connectivité, mais l'extrémité PE et l'entité P ne contiennent pas nécessairement l'information de connectivité.

B) *Calcul de trajet*

Un trajet peut être calculé par l'extrémité CE et spécifié, par exemple, à l'intérieur d'une demande de commande de connexion. Elle peut aussi être calculée par le contrôleur PCC.

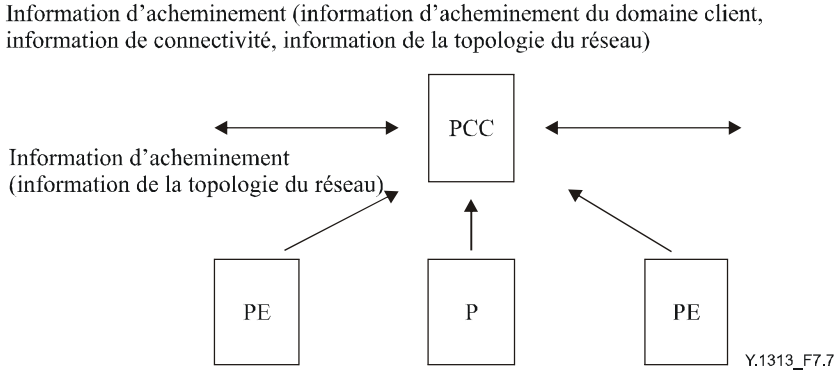

Figure 7-7/Y.1313 – Tenue à jour de l'information d'acheminement et calcul de trajet

• *Commande de connexion*

Le contrôleur PCC, l'extrémité PE et l'entité P contiennent l'information de commande de connexion. Le contrôleur PCC communique avec les entités clients pour recevoir les demandes de connexion après quoi, le contrôleur PCC communique avec les extrémités PE et les entités P pour établir les connexions. A noter que l'extrémité PE et l'entité P contiennent des informations de connexion nodale (information de brassage nodal, par exemple), mais ne contiennent pas nécessairement toute l'information de connexion (information explicite de trajet, par exemple).

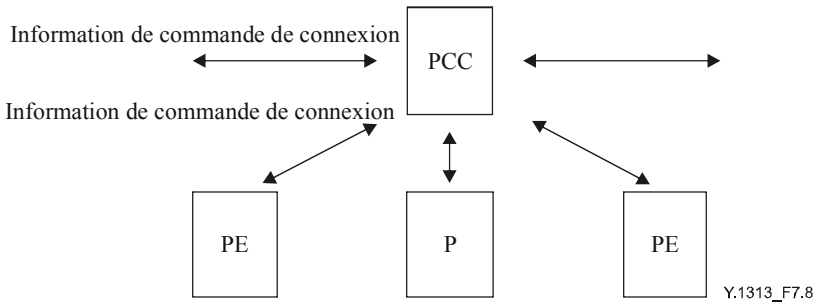

Figure 7-8/Y.1313 – Commande de connexion

3) Architecture hybride

Dans le cas d'une architecture hybride, certaines fonctions de tenue à jour des informations sur les membres, de tenue à jour des informations d'acheminement et de calcul de trajet, ainsi que de commande de connexion sont décentralisées alors que d'autres fonctions sont centralisées.

On distingue différents types d'architecture hybride. Essentiellement, dans le cas d'une architecture de réseau de fournisseur hybride, les fonctions permettant de communiquer avec les clients sont hybrides, ce qui signifie que certaines fonctions sont centralisées (c'est-à-dire les communications des contrôleurs PCC et CCC) tandis que d'autres sont décentralisées (c'est-à-dire les communications des extrémités PE et CE), et/ou des fonctions à l'intérieur du réseau du fournisseur (c'est-à-dire des communications PE/P et PCC) sont hybrides.

Un exemple est constitué par la décentralisation des fonctions dans lesquelles les fonctions propres au service VPN L1 telles que la tenue à jour des informations sur les membres, ainsi que les fonctions de gestion sont centralisées tandis que les fonctions communes permettant d'établir des connexions L1, telle la commande de connexion, sont décentralisées.

7.2 Architecture de réseau du client

1) Architecture décentralisée

Chaque extrémité CE possède une ou plusieurs entités qui assurent les fonctions de commande et l'extrémité CE est commandée par les entités correspondantes. Dans une architecture décentralisée, l'extrémité CE est l'entité qui permet de communiquer avec l'entité fournisseur, qui est en général l'extrémité PE.

Dans une architecture décentralisée, les fonctions de tenue à jour des informations sur les membres, de tenue à jour de l'information d'acheminement, de calcul de trajet et de commande de connexion sont décentralisées.

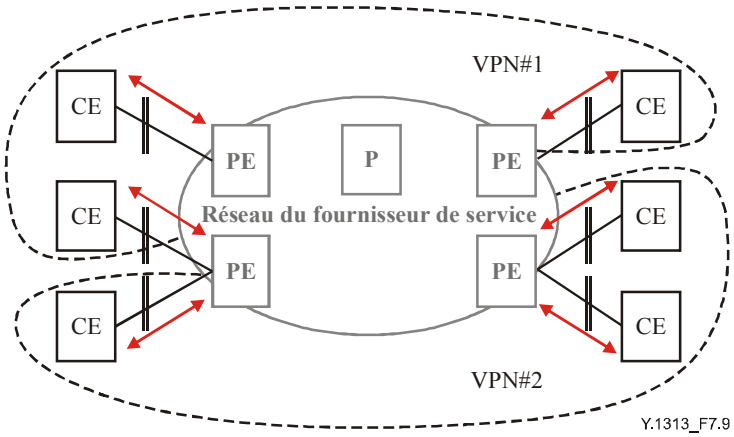

Figure 7-9/Y.1313 – Architecture décentralisée de réseau client VPN L1

2) Architecture centralisée

Une entité centralisée exécute les fonctions de commande requises au nom de plusieurs extrémités CE connectées au réseau du fournisseur.

Dans une architecture centralisée, un contrôleur centralisé du client (CCC) est l'entité qui permet de communiquer avec l'entité fournisseur, qui est en général le contrôleur PCC. Dans certains cas, le contrôleur CCC ne transmet que l'information de commande demandée des extrémités CE à l'entité du fournisseur. Dans d'autres cas, le contrôleur CCC peut participer aux fonctions de commande mais les extrémités CE ne permettent de recevoir que des connexions provenant d'autres extrémités CE tels les contrôleurs CCC qui reçoivent l'accès depuis les extrémités CE actives.

Dans une architecture centralisée, les fonctions de tenue à jour des informations sur les membres, de tenue à jour de l'information d'acheminement, et de calcul de trajet ainsi que de commande de connexion sont centralisées.

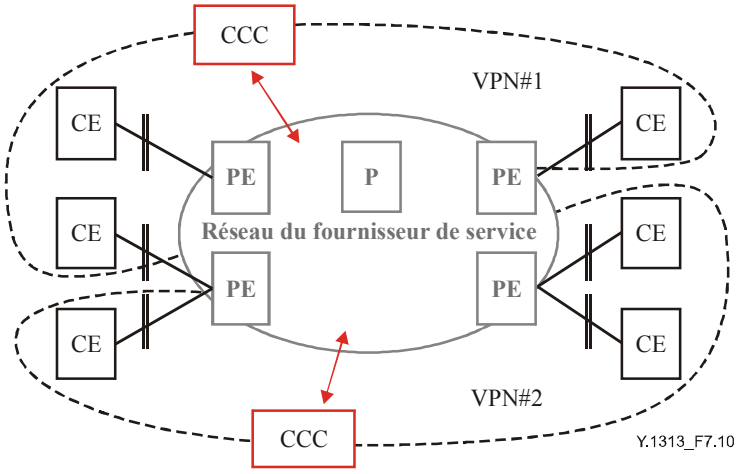

Figure 7-10/Y.1313 – Architecture centralisée de réseau client VPN L1

3) Architecture hybride

Dans une architecture hybride, certaines fonctions de tenue à jour des informations sur les membres, de tenue à jour de l'information d'acheminement, de calcul de trajet et de commande de connexion sont décentralisées, tandis que d'autres sont centralisées.

7.3 Architecture de gestion

On distingue deux aspects concernant la gestion, l'un est la gestion par le fournisseur et l'autre est la gestion par le client.

7.3.1 Architecture de gestion par le fournisseur

Certaines fonctions de gestion sont centralisées indépendamment du fait que sont centralisées ou non les fonctions de tenue à jour des informations sur les membres, de tenue à jour de l'information d'acheminement et de calcul de trajet ainsi que la commande de connexion. Parmi des exemples types, citons les fonctions d'autorisation et de comptabilité.

Les politiques comportent deux entités: une entité de décision et une autre de mise en application. La première est appelée point de décision de politique (PDP, *policy decision point*) et la seconde point d'application de la politique (PEP, *policy enforcement point*). Les points PDP et PEP peuvent être situés en des lieux différents du réseau.

Le Tableau 7-1 décrit un exemple type de la façon dont les fonctions de gestion sont distribuées, lorsque les fonctions de tenue à jour des informations sur les membres, de tenue à jour de l'information d'acheminement et de calcul de trajet ainsi que de commande de connexion sont décentralisées ou centralisées.

Tableau 7-1/Y.1313 – Distribution des fonctions de gestion

	Architecture décentralisée du réseau du fournisseur	**Architecture centralisée du réseau du fournisseur**
AAA	Centralisées (Note 1)	Centralisées
Politiques	PDP: décentralisé ou centralisé PEP: décentralisé	PDP: centralisé PEP: centralisé
OAM et gestion des anomalies	Décentralisées ou centralisées (Note 2)	Centralisées (Note 3)
NOTE 1 – L'authentification peut être décentralisée, ce qui signifie que les extrémités PE identifient les entités clients avec lesquelles elles communiquent. NOTE 2 – Certaines fonctions, telle la surveillance de la performance, peuvent toujours être décentralisées. NOTE 3 – Certaines fonctions, telles les fonctions de protection et de rétablissement, peuvent être décentralisées.		

7.3.2 Architecture de gestion client

Le client peut disposer d'une interface avec le système de gestion du fournisseur; à savoir l'interface de gestion du réseau par le client (CNM, *customer network management*). Le client peut déléguer des capacités de cette interface à une ou plusieurs de ses extrémités clients CE en partie ou en totalité. Ces interfaces sont décrites à la Figure 7-11.

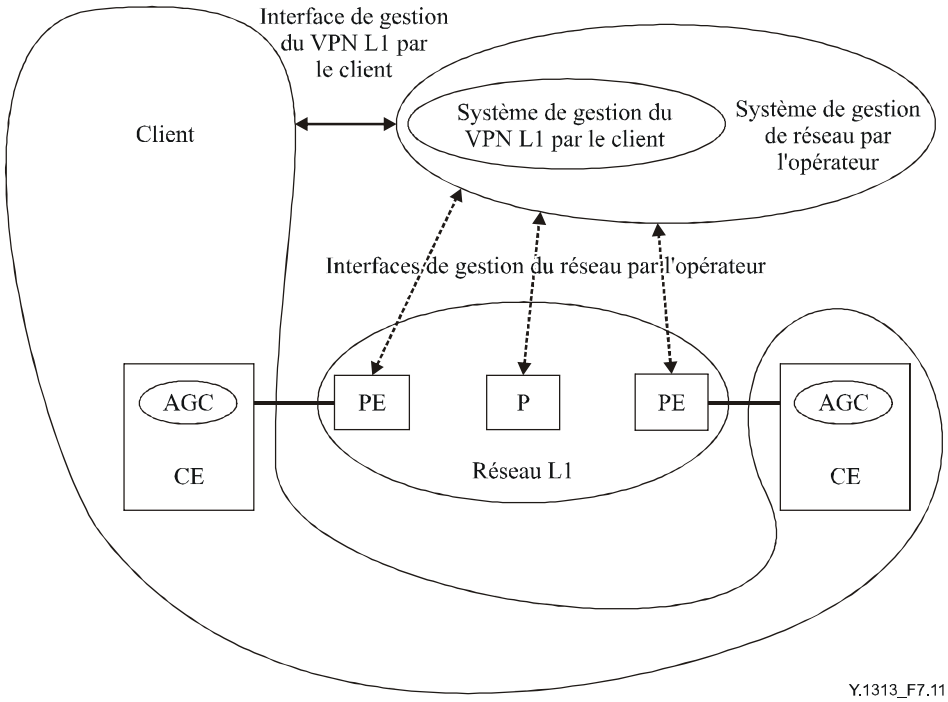

Figure 7-11/Y.1313 – Interfaces entre le client et le réseau

Les fonctions de l'interface CNM sont les suivantes:

- fonctionnalités analogues à celles de communication des contrôleurs PCC et CCC décrites au § 7.1, point 2). (C'est-à-dire demande de connexion reconfigurable PE-PE dans le réseau L1 du client, vue de la topologie des liaisons exclusivement attribuées au réseau VPN L1 du client, demande d'état des lignes exclusivement attribuées au réseau L1 VPN du client, interrogation sur l'état des informations sur les membres);
- authentification et autorisation de l'accès pour le client;
- demande de l'adjonction ou de la suppression d'une extrémité CE, une liaison partagée ou d'une liaison spécialisée;
- test des liaisons attribuées à titre exclusif au réseau VPN L1 du client;
- fixation des seuils pour les alertes de dépassement de seuil (TCA, *threshold crossing alerts*) pour les liaisons exclusivement attribuées à titre exclusif au réseau VPN L1 du client;
- signalisation des alarmes et des alertes TCA pour les liaisons exclusivement attribuées au réseau VPN L1 du client;
- interrogation et signalisation de l'information de performance des liaisons exclusivement attribuées à titre exclusif au réseau VPN L1 du client;
- traçage d'une connexion à travers le réseau VPN L1 du client;
- rapport d'information de facturation concernant le réseau VPN L1 du client.

8 Concepts d'architecture fonctionnelle de réseau VPN de couche 1

8.1 Structure architecturale

8.1.1 Structure du Plan U

Une connexion de liaison est une entité de transport capable de transférer l'information entre deux points de connexion (CP, *connection point*), un point de connexion correspondant à une fonction d'entrée-sortie de la connexion de liaison. Citons comme exemples de connexion de liaison, les connexions VC-3 et VC-4.

Une série de connexions de liaison contiguës et de connexions de sous-réseaux peuvent être regroupées pour former une liaison composite série. Dans la présente Recommandation, le terme liaison servira souvent à désigner une liaison composite série. A noter que la matrice de commutation d'un brasseur constitue un exemple de sous-réseau.

Plusieurs connexions de liaison avec des points CP situés dans les deux mêmes sous-réseaux peuvent être regroupées en parallèle. On appelle ce regroupement un faisceau de liaisons.

Les liaisons sont construites sur la base des cheminements de la couche serveur dans le Plan U. Les liaisons sont en fait les vecteurs qui permettent d'assurer les fonctions de gestion de réseau VPN de couche 1, en particulier la gestion des anomalies et de la performance.

8.1.2 Structure du Plan C

Une connexion de liaison de point de sous-réseau (SNP, *subnetwork point*) est une relation de commande entre deux points SNP. Les points SNP sont des entités du Plan C qui sont liés aux points CP du Plan U. Les connexions de liaison SNP servent à l'acheminement et contrairement aux liaisons, elles ne peuvent transférer des informations par elles-mêmes.

Toutes les associations possibles SNP-CP sont déterminées par la configuration, tandis que les associations réelles sont déterminées à l'instant où une connexion a été établie. Lorsqu'un point SNP devient lié à un point CP, les liaisons correspondantes deviennent également liées.

Les connexions de liaison SNP multiples avec des points SNP situés dans deux mêmes réseaux peuvent être regroupées en parallèle pour former une liaison de pool de points de sous-réseau (SNPP, *subnetwork point pool*). Toutes les connexions de liaison SNP d'une liaison SNPP sont traitées de manière égale pour l'acheminement (en termes équivalents GMPLS, une liaison SNPP correspond à une liaison TE).

De plus, la Rec. UIT-T Y.1311 ne porte que sur des réseaux "équipés d'accès". Dans cette architecture, les réseaux VPN de couche 1 sont également équipés d'accès, ceux-ci apparaissant sous forme de pools SNPP.

8.1.3 Structure du Plan M

Les structures du Plan U et du Plan C définies ci-dessous sont accessibles dans le Plan M. Il en résulte que le Plan M a deux vues différentes, mais liées, des ressources de réseau à savoir une vue dans le Plan C et une vue dans le Plan U comme le montre la Figure 8-1.

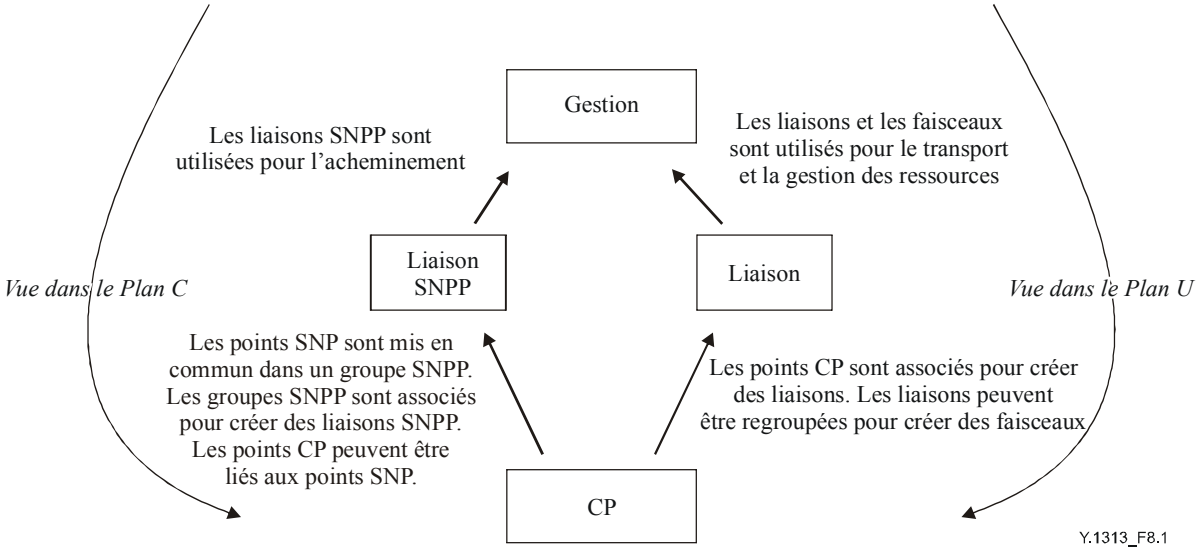

Figure 8-1/Y.1313 – Liaisons pour le Plan U et liaisons SNPP pour le Plan C

8.2 Schémas d'attribution des ressources

8.2.1 Plan U partagé et Plan U exclusif

L'architecture de service des réseaux VPN de couche 1 décrite dans la Rec. UIT-T Y.1312, exige la prise en charge des ressources du Plan U partagé et des ressources du Plan U exclusif. Par ressources du Plan U partagé, on entend partage dans le temps des ressources utilisées par plusieurs réseaux VPN. Par ressources du Plan U exclusif on entend des ressources attribuées exclusivement à un réseau VPN et pour toute sa durée de vie.

Du point de vue des structures du Plan U, une liaison partagée est une liaison configurée pour être utilisée par plusieurs réseaux VPN de couche 1 donnés. Une liaison exclusive est une liaison configurée pour être utilisée par un seul et unique réseau VPN de couche 1.

Du point de vue des structures du Plan C, une liaison SNPP doit être configurée pour être utilisée uniquement par un réseau VPN de couche 1; en d'autres termes, les liaisons SNPP ne sont pas partagées. Les points SNP d'un pool SNPP assignés à un réseau VPN de couche 1 peuvent être uniquement associés aux points CP assignés au même réseau VPN de couche 1 sur une base partagée ou exclusive.

Il existe toutefois un cas spécial, celui d'une liaison publiquement partagée, c'est-à-dire une liaison configurée pour être utilisée par un réseau quelconque VPN de couche 1. Si un pool SNPP n'a pas été assigné à un réseau VPN de couche 1, les points SNP peuvent être uniquement associés à des points CP publiquement partagés. Cela garantit la compatibilité avec les liaisons VPN autres que de couche 1.

A noter que cette notion s'applique non seulement dans le cadre du réseau du fournisseur, mais également entre l'extrémité CE et l'extrémité PE.

La Figure 8-2 décrit un exemple avec deux réseaux VPN de couche 1. Les réseaux VPN de couche 1 désignés par A et B disposent chacun de deux points CP exclusifs. Ces deux réseaux VPN de couche 1 partagent deux points CP. Dans le dernier cas, l'association d'un point CP avec un point SNP dans un réseau VPN de couche 1 ne sera pas possible si le point CP est déjà associé à un autre point SNP de l'autre réseau VPN de couche 1 – le premier point SNP est dans ce cas déclaré occupé.

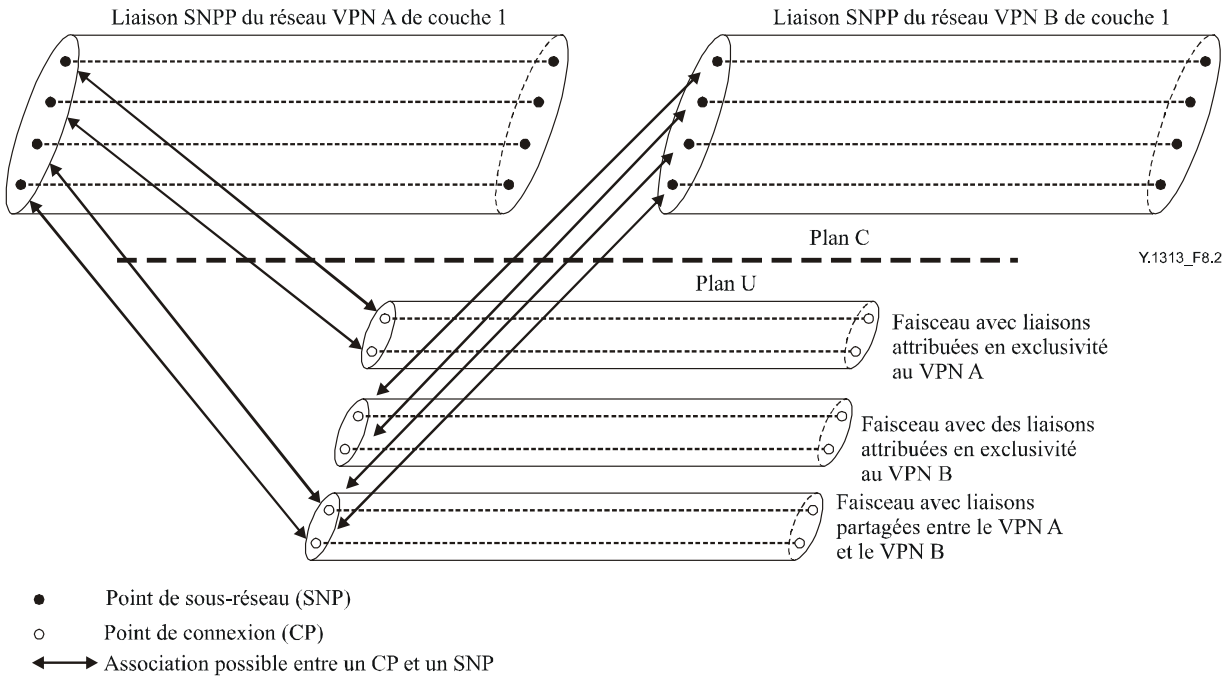

Figure 8-2/Y.1313 – Relation entre les points CP du Plan U et les points SNP du Plan C

8.2.2 Plan C partagé ou Plan C exclusif

On distingue deux formes d'attribution des ressources du Plan C pour chaque réseau VPN, à savoir l'attribution partagée et l'attribution exclusive tel que décrit dans la Rec. UIT-T Y.1312. Dans le cas de ressources exclusives du Plan C, différentes ressources du Plan C sont attribuées à différents réseaux VPN, tandis que dans le cas de ressources partagées du Plan C, les mêmes ressources du Plan C peuvent être utilisées par plusieurs réseaux VPN.

1) Plan C exclusif

Sous cette forme, les ressources du Plan U sont en général exclusives, et les informations de disponibilité de ressource du domaine client et du domaine fournisseur peuvent être échangées entre le client et le réseau, ce qui permet aux clients de faire leur propre sélection de liaison parmi les ressources du Plan U exclusif, tel que décrit dans la Rec. UIT-T Y.1312. Dans le cas présent, les informations sur la disponibilité de ressource du fournisseur peuvent être résumées, dans le sens où les clients ne peuvent pas recevoir exactement les mêmes informations concernant les ressources du Plan U qui sont attribuées en exclusivité dans le réseau du fournisseur. Le niveau d'abstraction peut varier en fonction du contrat de service entre le client et le fournisseur. A noter qu'il peut y avoir un contrat de service dans lequel tout le réseau du fournisseur peut être considéré comme un seul nœud.

Une façon d'implémenter un Plan C exclusif consiste à attribuer différentes instances et bases de données à chaque réseau VPN, comme par exemple un routeur virtuel. Les bases de données contenant les informations sur les membres, l'information d'acheminement et de commande de connexion, ainsi que les politiques, sont de titre exclusif. Les clients communiquent avec des instances attribuées à titre exclusif pour échanger les informations sur les membres, les informations d'acheminement et les informations de commande de connexion.

Pour retransmettre l'information reçue en provenance des clients, le réseau doit disposer d'une fonction permettant d'identifier le réseau VPN auquel l'information doit appartenir. Les méthodes permettant de lever les ambiguïtés mentionnées au § 8.3.2 peuvent être utilisées à cette fin.

Dans le réseau du fournisseur, les instances et les bases de données partagées pourraient être utilisées. Dans ce cas, on s'attend à ce qu'il y ait échange d'informations entre les bases de données/instances exclusives et les bases de données/instances partagées. La traduction des adresses peut être nécessaire tout comme le filtrage de l'information en provenance des bases de données partagées vers les bases de données exclusives.

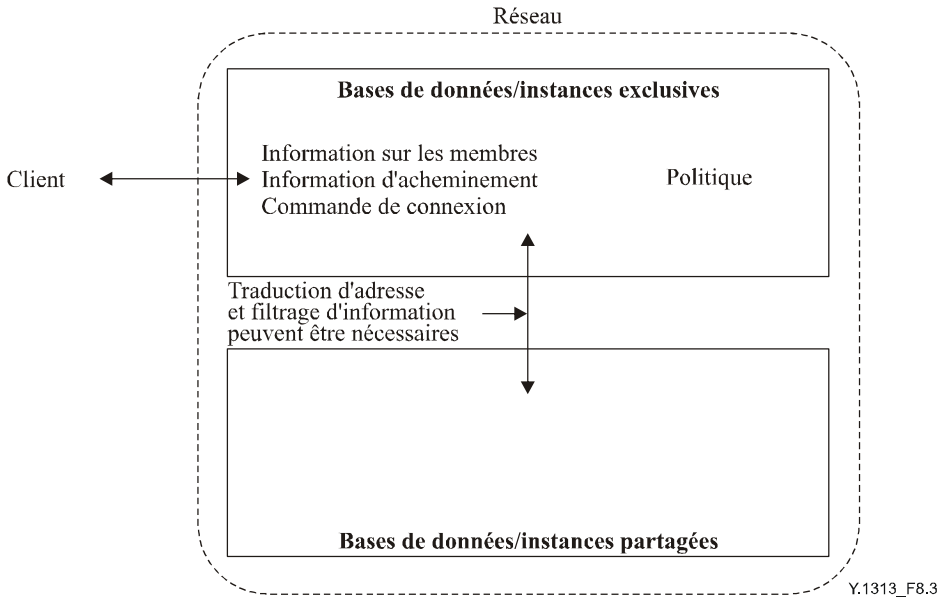

Figure 8-3/Y.1313 – Exemple de Plan C exclusif

Un autre type de ressource du Plan C est constitué par les liaisons de commande. Les liaisons de commande sont utilisées pour le transfert des messages de commande associés à la gestion des ressources, à la tenue à jour des informations sur les membres, à l'information d'acheminement et à la commande de connexion. Une liaison de commande peut être exclusivement affectée à un réseau VPN de couche 1.

2) Plan C partagé

Dans le Plan C partagé, l'espace adresse est commun à tous les réseaux VPN dans le réseau du fournisseur.

Sous cette forme, les ressources du Plan U sont attribuées à titre exclusif ou partagées.

Une façon d'implémenter le Plan C partagé est d'attribuer la même instance et la même base de données à tous les réseaux VPN. Toutefois, les informations sur les membres et la politique sont toujours attribuées à titre exclusif, comme décrit dans la Rec. UIT-T Y.1312.

A noter que même si des instances d'acheminement sont partagées, il est toujours possible d'affecter en exclusivité des ressources du Plan C en utilisant un mécanisme tel que le coloriage. Dans ce cas, les ressources du Plan U attribuées à titre exclusif à un réseau VPN sont utilisées dans le processus de sélection de liaison.

Des bases de données et des instances partagées sont utilisées dans le réseau du fournisseur. Dans ce cas l'échange d'informations entre les bases de données/instances de type exclusif et les bases de données/instances partagées est attendu. La traduction des adresses peut être nécessaire tout comme le filtrage de l'information en provenance des bases de données partagées vers les bases de données exclusives.

Etant donné que l'espace adresse est commun pour les réseaux VPN dans le réseau du fournisseur, et s'il n'existe pas de mécanisme permettant d'identifier le réseau VPN auquel doit appartenir

l'information reçue en provenance des clients, une adresse publique doit être assignée pour identifier une liaison CE-PE du pool SNPP. Toutefois, des adresses privées peuvent être utilisées dans le site du client. Une demande de connexion est reçue par les fonctions de commande de connexion, suivie d'une restriction de connectivité fondée sur les informations sur les membres.

Par ailleurs, lorsqu'il existe un mécanisme permettant d'identifier le réseau VPN auquel appartient l'information reçue en provenance des clients, telles des méthodes de levée d'ambiguïté d'adresse mentionnées au § 8.3.2, en utilisant une table de traduction d'adresses par réseau VPN, des adresses privées peuvent être utilisées.

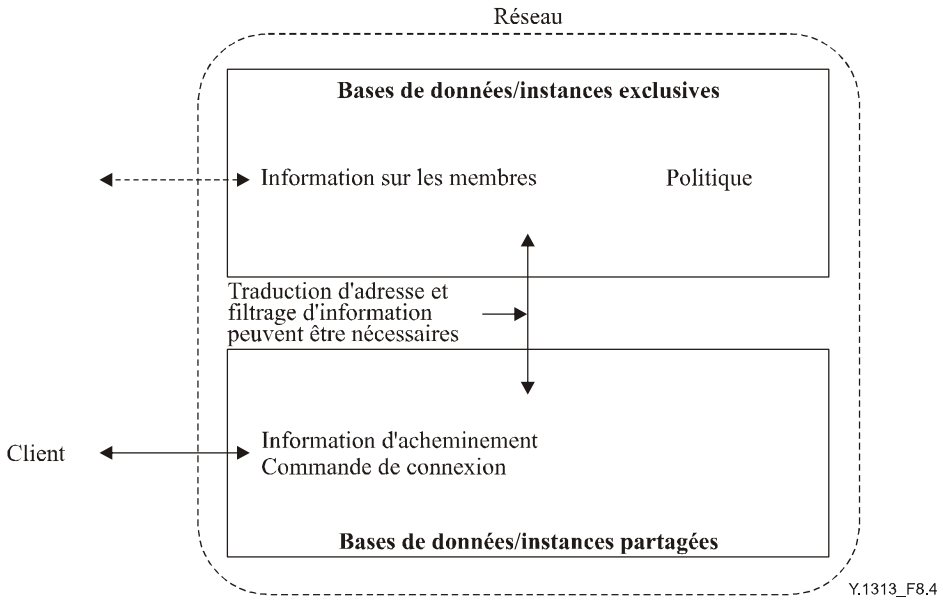

Figure 8-4/Y.1313 – Exemple de Plan C partagé

Une liaison de commande est un autre type de ressource du Plan C qui peut être partagé entre plusieurs VPN de couche 1. Les messages de commande reçus à travers une liaison de commande partagée via une interface CE-PE doivent faire l'objet d'une levée d'ambiguïté en ce qui concerne le réseau VPN de couche 1 auquel ils s'appliquent. Cette levée d'ambiguïté doit être effectuée en faisant référence explicite à un réseau VPN de couche 1 dans le message de commande ou en indiquant une adresse publique.

8.3 Adressage privé

8.3.1 Prescriptions

Dans un réseau VPN de couche 1, chaque liaison CE-PE de pool SNPP doit avoir une adresse unique dans le contexte du réseau VPN conformément à la Rec. UIT-T Y.1312. Cette adresse peut être une adresse publique assignée par l'opérateur du réseau du fournisseur ou une adresse privée assignée par le client. Dans ce dernier cas, le réseau du fournisseur peut traduire l'adresse privée en une adresse publique afin de prendre en charge la commande de connexion dans le réseau du fournisseur.

8.3.2 Contextes permettant de lever l'ambiguïté des adresses privées

Contrairement aux adresses publiques, les adresses privées de réseau VPN de couche 1 peuvent présenter un certain chevauchement et il est essentiel que le fournisseur soit en mesure de lever cette ambiguïté, c'est-à-dire de déterminer à quel espace adresse VPN de couche 1 elles appartiennent. On distingue deux méthodes générales de levée d'ambiguïté des adresses VPN de couche 1: la méthode implicite et la méthode explicite.

La méthode implicite fait intervenir l'affectation exclusive d'une liaison de commande à chaque réseau VPN de couche 1. Etant donné que la liaison de commande relève d'une relation univoque, avec un réseau VPN de couche 1, l'adresse privée contenue dans les messages envoyés sur cette liaison de commande sera interprétée dans le contexte de ce réseau VPN de couche 1. Il n'est pas nécessaire de faire référence explicite au réseau VPN de couche 1 dans les messages de commande.

Dans la méthode explicite, on suppose que la liaison de commande est partagée entre les réseaux VPN de couche 1. Dans ce cas, la levée d'ambiguïté doit être effectuée explicitement par le fournisseur. On peut pour cela utiliser des messages de commande d'étiquetage avec un identificateur de réseaux VPN de couche 1 globalement unique.

8.3.3 Traduction d'adresse

Dans le cas où les adresses privées VPN de couche 1 doivent être traduites en adresses publiques, l'entité fournisseur devra formuler une requête à un annuaire. L'annuaire est essentiellement une base de données qui peut être répartie entre toutes les extrémités PE ou centralisée dans le réseau.

9 Architecture des entités fonctionnelles VPN de couche 1

9.1 Tenue à jour des informations sur les membres et gestion des politiques relatives à la connectivité

Par informations sur les membres on entend une liste d'extrémités CE situées dans le même réseau VPN. Les informations sur les membres sont tenues à jour dans le réseau du fournisseur et la connectivité entre extrémités CE est limitée en tenant compte des informations sur les membres. Au contraire, il est parfois exigé de limiter la connectivité même à l'intérieur du même réseau VPN. Dans ce cas, la limitation de connectivité basée sur la politique de connectivité pour chaque réseau VPN doit être gérée.

9.1.1 Tenue à jour des informations sur les membres

Les informations sur les membres sont constituées par une liste d'extrémités CE situées dans un même réseau VPN. Dans des descriptions plus détaillées, les informations sur les membres peuvent être représentées sous forme d'une liste de noms SNPP CE-PE à l'intérieur du même réseau VPN. Le fournisseur doit tenir à jour les informations sur les membres.

La connectivité doit être limitée sur la base des informations sur les membres, qui permettent de limiter la connectivité uniquement à l'intérieur du même réseau VPN. Dans une architecture décentralisée de réseau du fournisseur, les informations sur les membres doivent être réparties dans chaque extrémité PE, et si possible en recourant à des mécanismes automatiques.

A l'intérieur du réseau du fournisseur, les informations sur les membres doivent être tenues à jour en associant des identificateurs d'extrémité PE à des noms SNPP CE-PE. Ces informations peuvent être utilisées pour identifier un point de sortie d'un réseau de fournisseur approprié pour l'acheminement des connexions.

Le mécanisme utilisé pour répartir et tenir à jour les informations sur les membres et le mécanisme utilisé pour répartir et maintenir les informations relatives à la politique de connectivité peuvent être le même.

9.1.2 Gestion de la politique de connectivité

9.1.2.1 Prescriptions

Dans la Rec. UIT-T Y.1312 sont décrites un certain nombre de prescriptions relatives aux politiques de connectivité. Ces politiques spécifient le membre d'un réseau VPN L1 qui est habilité à établir à tout moment des connexions avec d'autres membres spécifiés du réseau VPN L1.

9.1.2.2 Politiques de connectivité

Le contrôle d'admission des demandes de connexion peut être effectué sur la base des politiques de connectivité configurées pour une extrémité CE donnée dans un réseau VPN L1 donné. Le contrôle d'admission des demandes de connexion VPN L1 est pris en charge par une entité du fournisseur tel que défini dans la Rec. UIT-T Y.1312.

Les politiques de connectivité peuvent être consignées dans deux listes d'adresses pour chaque réseau VPN L1: une liste d'adresses de demandes de connexion sortante admissible et une liste d'adresses de demandes de connexion entrante admissible.

Si une entité fournisseur reçoit une demande de connexion sortante VPN L1, d'une entité client VPN L1 vers le fournisseur, comportant une adresse de destination qui n'apparaît pas dans la liste des adresses de demandes de connexion sortante admissible pour le réseau VPN L1 considéré, cette entité fournisseur rejette cette demande de connexion. Si une entité fournisseur reçoit une demande de connexion entrante VPN L1, du fournisseur à une entité client VPN L1, comportant une adresse source qui n'apparaît pas dans la liste d'adresses de demandes de connexion entrante admissible pour le réseau VPN L1 considéré, cette entité fournisseur rejette cette demande de connexion. L'utilisation de deux listes d'adresses de demandes de connexion admissible entrante et sortante permet l'existence de politiques de connectivité asymétrique parmi les membres du réseau VPN L1, ce qu'illustre la Figure 9-1.

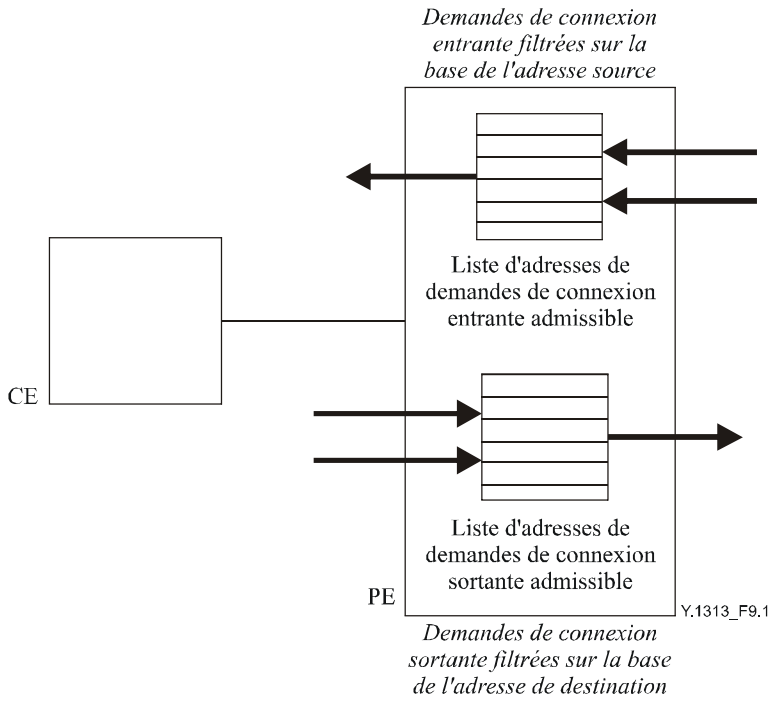

Figure 9-1/Y.1313 – Contrôle d'admission de demandes de connexion entrante et sortante

9.1.2.3 Configuration des politiques de connectivité

Dans l'architecture décentralisée des réseaux des fournisseurs, les listes d'adresses de demandes de connexion admissible sortante et entrante pour chaque réseau VPN L1 sur chaque extrémité PE doivent être remplies et tenues à jour. Les règles applicables sont les suivantes:

1) la liste d'adresses de demandes de connexion entrante admissible est toujours configurée;

2) la liste d'adresses de demandes de connexion sortante admissible peut être statiquement configurée ou bien automatiquement établie et dynamiquement tenue à jour. Ce dernier mode permet la fourniture à une seule extrémité, des listes d'adresses de demandes de connexion admissible.

A noter que lorsque les deux listes sont statiquement configurées, la solution est donc analogue aux groupes fermés d'utilisateurs (CUG, *closed user group*).

9.1.2.4 Echange d'informations entre extrémités PE et le CE concernant la politique de connectivité du réseau VPN L1

La gestion de la politique de connectivité entre extrémités PE a été décrite dans les précédents paragraphes. La gestion de politique de connectivité peut être étendue à l'interface CE-PE en tant que service supplémentaire. On distingue deux cas pour ce service:

1) l'extrémité CE peut demander à l'extrémité PE de modifier la configuration de sa liste d'adresses de demandes de connexion entrante admissible. Cela déclenchera, entre autres, la tenue à jour dynamique des listes d'adresses sortantes admissibles;
2) l'extrémité PE peut transmettre une liste d'adresses de demandes de connexion sortante admissible mise à jour à l'extrémité CE après réception d'un message de tenue à jour dynamique.

9.2 Tenue à jour de l'information d'acheminement et calcul de trajet

On distingue deux aspects concernant la tenue à jour de l'information d'acheminement et le calcul de trajet. L'un se situe entre le client et le réseau et l'autre à l'intérieur du réseau.

1) Entre le client et le réseau

Si les clients sont autorisés à demander des connexions et à inclure un trajet explicite dans cette demande, l'information relative à la topologie et à l'état doit être fournie à temps pour permettre au client de calculer le trajet. Dans ce cas, dans une architecture décentralisée, le canal de commande CE-PE doit prendre en charge à la fois une signalisation et un protocole d'acheminement. L'information d'acheminement doit être limitée aux ressources fournies dans le cadre du service VPN L1.

On distingue deux types d'acheminement: l'acheminement unidirectionnel et l'acheminement bidirectionnel. Dans l'acheminement unidirectionnel, l'information de topologie du réseau VPN L1 est transmise de l'extrémité PE à l'extrémité CE. En outre, l'information de connectivité peut être transmise de l'extrémité PE à l'extrémité CE. Dans le cas de l'acheminement bidirectionnel, l'information de topologie des réseaux du client est également transmise de l'extrémité CE à l'extrémité PE, dans la mesure où cette topologie concerne le réseau VPN L1. On trouvera au § 5 une description plus détaillée de la topologie et de l'information de connectivité.

A noter que le transfert transparent de l'information entre des entités clients dans le réseau VPN L1 peut être utilisé pour acheminer l'information d'acheminement du domaine client.

2) A l'intérieur du réseau

L'information d'acheminement est utilisée pour acheminer une connexion. L'information d'acheminement du domaine client peut être utilisée afin d'optimiser le calcul de trajet. Un trajet est calculé sur la base de la disponibilité des ressources réseau obtenue au moyen du mécanisme de tenue à jour de l'information d'acheminement, de la politique du fournisseur de réseaux et de la politique du client (politique par réseau VPN). En particulier, le calcul de trajet diffère selon la manière dont les ressources du Plan U sont attribuées. Lorsque les ressources du Plan U sont attribuées à titre exclusif, le calcul de trajet est effectué de manière à ce que seule la partie des ressources attribuées à titre exclusif est utilisée. Par ailleurs, lorsque les ressources du Plan U sont

partagées, le calcul de trajet est effectué de manière à ce que les ressources puissent être utilisées par plusieurs réseaux VPN.

A noter que lorsque l'information d'acheminement a été échangée entre le client et le réseau, les clients peuvent spécifier un trajet explicite, tel que décrit au § 9.3. Dans ce cas, il n'est pas nécessaire pour le réseau d'effectuer le calcul de trajet.

9.3 Commande de connexion

La commande de connexion nécessite la présence de deux fonctionnalités. Premièrement les demandes de connexion peuvent inclure des adresses privées de réseaux VPN L1 pour l'origine et la destination. Deuxièmement, les demandes de connexion peuvent inclure un trajet explicite à utiliser pour la connexion. Des informations au sujet de ces trajets explicites sont disponibles grâce à l'échange d'informations d'acheminement décrit ci-dessus.

9.4 Gestion

On distingue deux aspects en gestion. Le premier est la gestion par le fournisseur et l'autre est la gestion par le client, tels que décrits au § 7.3. La gestion par la fournisseur doit garantir un fonctionnement sûr, fiable et tolérant aux anomalies du réseau. La gestion par le fournisseur traite également de fonctions propres aux services, tels l'AAA et les politiques par réseaux VPN.

En même temps, le client peut accéder aux capacités de gestion par l'interface CNM. L'interface CNM permet aux clients de gérer la partie exclusive du réseau du fournisseur.

De plus, les capacités de gestion doivent permettre de prendre en charge deux vues différentes mais liées des ressources du réseau, une vue dans le Plan C et une vue dans le Plan U, telles que décrites au § 8.1.3.

10 Exemples d'architecture fonctionnelle

10.1 Architecture décentralisée du réseau du fournisseur

Sont décrits ci-après trois exemples détaillés d'architecture décentralisée de réseau du fournisseur sur la base des critères de classification architecturale indiqués aux § 7 et 8.

1) Plan C exclusif

Des instances et des bases de données sont attribuées à titre exclusif pour chaque réseau VPN dans l'extrémité PE et l'entité P. Les canaux de communication entre des instances attribuées à titre exclusif peuvent être établis en séparant logiquement le canal de communication commun.

Perspective service: l'information d'acheminement peut être fournie aux clients. Des adresses privées peuvent être facilement prises en charge. Aucun mécanisme de traduction d'adresse n'est nécessaire.

Tenue à jour des informations sur les membres: les informations sur les membres peuvent être intégrées à l'information d'acheminement décrite ci-dessous. L'information de politique de connectivité peut être acheminée de la même façon.

Tenue à jour des informations d'acheminement et calcul de trajet: la même instance peut être utilisée pour l'information d'acheminement du domaine client, information de topologie du réseau et l'information de connectivité. Dans ce cas, l'information de topologie du réseau associée en exclusivité à chaque réseau VPN est échangée par chaque instance exclusive. De même, le même mécanisme ou protocole peut être utilisé dans le réseau et entre le client et l'extrémité PE. Un trajet peut être calculé par l'extrémité CE et spécifié dans une demande de commande de connexion. Un trajet peut aussi être calculé par l'extrémité PE ou par l'extrémité PE et l'entité P.

Commande de connexion: le même mécanisme ou protocole peut être utilisé dans le réseau et entre le client et l'extrémité PE. Une seule session peut être établie entre les extrémités CE.

Gestion: certaines fonctions sont exécutées de manière décentralisée telle que décrite au § 7.3.

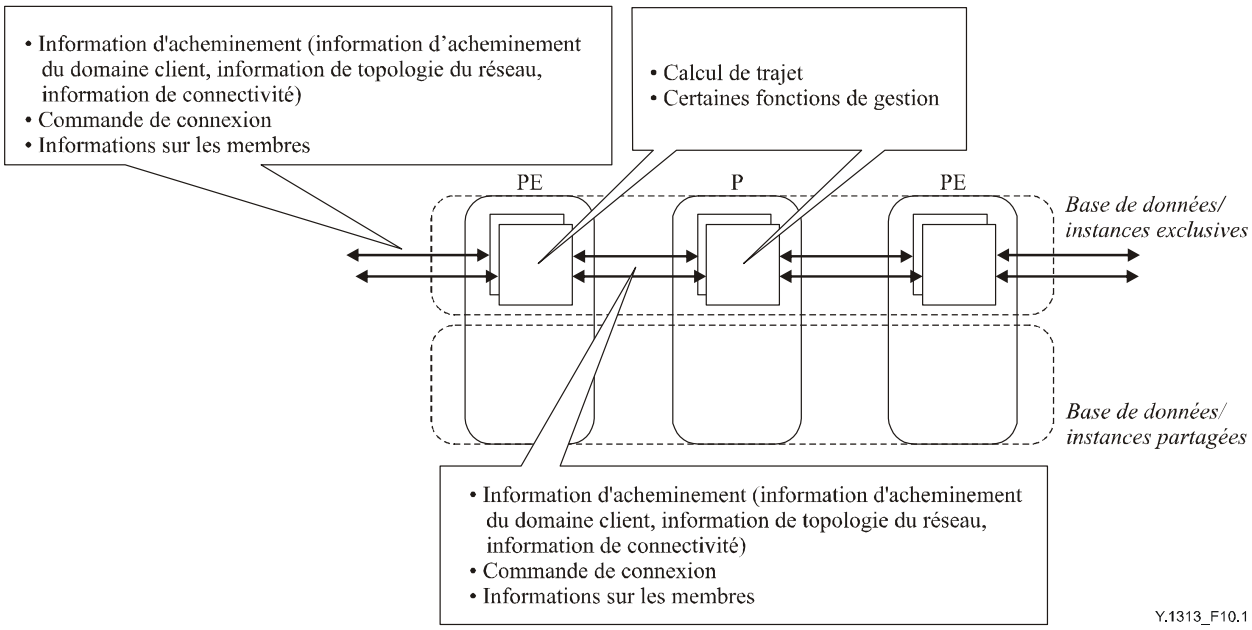

Figure 10-1/Y.1313 – Plan C exclusif

2) Plan C attribué en exclusivité dans l'extrémité PE

Les instances et les bases de données sont attribuées à titre exclusif à l'extrémité PE mais partagées dans l'entité P. Les canaux de communication entre les instances/bases de données attribuées à titre exclusif dans les extrémités PE sont établis, par exemple, par un mécanisme de tunnel. Ce canal de communication achemine l'information, telles les informations sur les membres, l'information d'acheminement du domaine client et l'information de connectivité. Les informations telles que la commande de connexion et l'information de topologie du réseau sont échangées entre des bases de données/instances partagées et attribuées à titre exclusif.

Perspective service: l'information d'acheminement peut être fournie aux clients. Une traduction d'adresse est nécessaire pour la prise en charge des adresses privées.

Tenue à jour des informations sur les membres: les informations sur les membres sont échangées par le canal de communication entre des instances/bases de données attribuées à titre exclusif dans les extrémités PE. Les informations sur les membres peuvent être insérées dans l'information d'acheminement décrite ci-dessous. A noter que les informations sur les membres peuvent être transmises à la base de données/instance partagée et non pas directement transférées vers l'extrémité PE distante. Les informations sur les membres sont alors transférées vers la base de données/instance partagée de l'extrémité PE distante via un canal de communication entre extrémités PE. L'information de politique de connectivité peut être acheminée de la même manière.

Tenue à jour des informations d'acheminement et calcul de trajet: l'information d'acheminement du domaine client et l'information de connectivité sont échangées via un canal de communication entre les instances/bases de données attribuées à titre exclusif dans les extrémités PE. L'information de topologie du réseau est transférée depuis la base de données/instance partagée vers des bases de données/instances attribuées à titre exclusif dans les extrémités PE. L'information de topologie du réseau échangée entre des instances partagées concerne tout le réseau, tandis que l'information de topologie du réseau est transférée depuis la base de données/instance partagée vers des bases de données/instances attribuées à titre exclusif au niveau des extrémités PE pour chaque

réseau VPN. A noter qu'il est moins probable que l'information d'acheminement du domaine client soit transférée vers la base de données/l'instance partagée et non pas directement transférée vers l'extrémité PE distante. Cela pose un problème de modularité. Tout comme l'information d'acheminement du domaine client et l'information de connectivité, le même mécanisme ou protocole pourrait être utilisé dans le réseau et entre le réseau et le client. De même que pour l'information de topologie du réseau, différents mécanismes ou protocoles pourraient être utilisés dans le réseau et entre le réseau et le fournisseur. Un trajet peut être calculé par l'extrémité CE et spécifié dans l'information de commande de connexion. Ou bien un trajet peut être calculé par l'extrémité PE ou par l'extrémité PE et l'entité P.

Commande de connexion: des mécanismes ou des protocoles dans le réseau et entre le réseau et le client peuvent être les mêmes ou être différents. Toutefois, une session unique ou plusieurs sessions (par exemple, une session CE-PE et une session PE-PE) peuvent être mises en place entre des extrémités CE.

Gestion: certaines fonctions sont exécutées de manière décentralisée comme décrit au § 7.3.

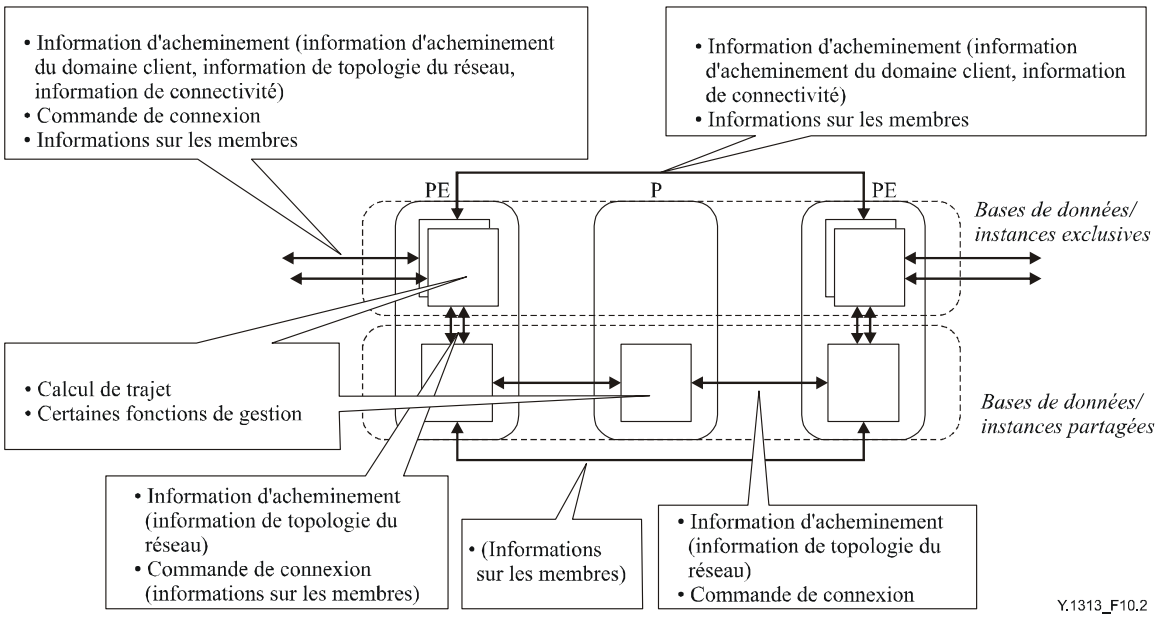

Figure 10-2/Y.1313 – Plan C attribué en exclusivité dans l'extrémité PE

3) Plan C partagé

Essentiellement, des instances/bases de données sont partagées dans l'extrémité PE et l'entité P, sauf les informations sur les membres et la politique. Un canal de communication est créé entre des instances/bases de données partagées dans les extrémités PE, susceptibles d'acheminer les informations sur les membres.

Perspective service: l'information d'acheminement peut ne pas être fournie aux clients, alors que la commande de connexion est fournie aux clients. Pour pouvoir prendre en charge des adresses privées spécifiant une liaison SNPP-CE-PE, une traduction d'adresse est nécessaire.

Tenue à jour des informations sur les membres: les informations sur les membres sont transférées sur un canal de communication connectant les Plans C partagés des extrémités PE distantes. Les informations sur les membres sont alors transférées vers les bases de données attribuées à titre exclusif. Les informations sur les membres peuvent être intégrées dans l'information d'acheminement décrite ci-dessous. L'information de politique de connectivité peut être acheminée de la même manière.

Tenue à jour des informations d'acheminement et calcul de trajet: l'information d'acheminement n'est pas fournie aux clients. Les clients spécifient l'adresse de la liaison SNPP-CE-PE ensuite, un trajet est calculé par l'extrémité PE, ou par l'extrémité PE et l'entité P.

Commande de connexion: une ou plusieurs sessions peuvent être établies entre extrémités CE.

Gestion: certaines fonctions sont exécutées de manière décentralisée comme décrit au § 7.3.

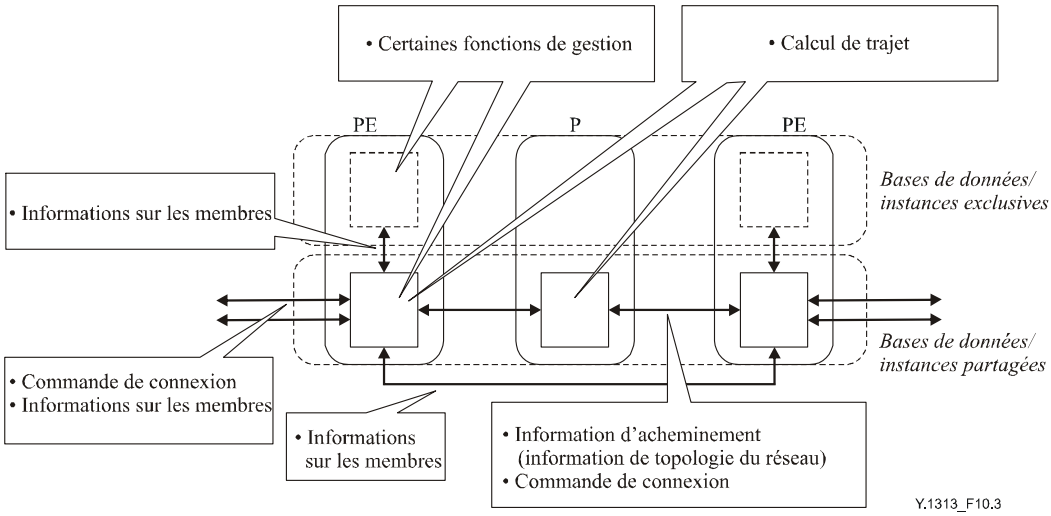

Figure 10-3/Y.1313 – Plan C partagé

10.2 Architecture hybride du réseau du fournisseur

Un exemple d'architecture hybride de réseau du fournisseur est celui où il y a décentralisation des fonctions et où certaines des fonctions de service propres au réseau VPN L1, telle la tenue à jour des informations sur les membres, ainsi que les fonctions de gestion sont centralisées alors que des fonctions communes établissant les connexions L1, telle la commande de connexion, sont décentralisées comme le montre la Figure 10-4.

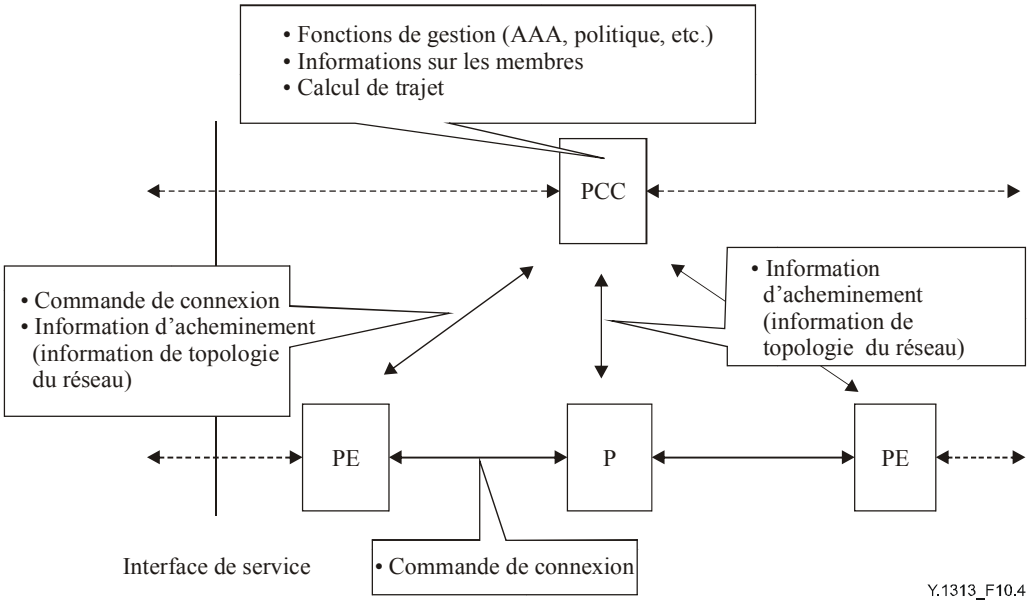

Figure 10-4/Y.1313 – Architecture hybride de réseau du fournisseur

Dans l'architecture hybride de réseau du fournisseur, le contrôleur PCC exécute une grande partie du processus de décision. Le contrôleur PCC exécute des fonctions inclues dans la restriction de connectivité en utilisant les informations sur les membres, une vérification de politique par réseau VPN et le calcul de trajet en utilisant l'information de topologie. Le contrôleur PCC exécute également les fonctions AAA. Après calcul d'un trajet, le contrôleur PCC communique avec une extrémité PE pour établir une connexion. Une connexion est établie par les fonctions décentralisées de commandes de connexion. Le contrôleur PCC peut avoir un Plan C exclusif.

Une autre fonctionnalité notable de l'architecture hybride de réseau du fournisseur est qu'il est tout aussi facile de communiquer avec les entités clients de manière décentralisée que de manière centralisée. Dans le premier cas, l'extrémité PE communique avec l'entité client, qui est très probablement l'extrémité CE. Dans le deuxième cas, le contrôleur PCC communique avec l'entité client qui est très probablement le contrôleur CCC.

En communiquant avec les extrémités PE et les entités P pour obtenir l'information de topologie, éventuellement en distribuant des fonctions d'acheminement, le contrôleur PCC peut disposer d'une information de topologie homogène avec les extrémités PE et les entités P.

1) Communication décentralisée avec le client

Dans ce modèle, l'extrémité PE communique avec les entités clients, telles les extrémités CE. L'extrémité PE reçoit une demande de connexion émanant d'un client, et transmet l'information de demande de connexion au contrôleur PCC. Le contrôleur PCC s'assure que l'établissement d'une connexion est autorisé en procédant à un contrôle de restriction de connectivité et à un contrôle de la classe de service. Le contrôleur PCC calcule ensuite un trajet et renvoie le résultat de son calcul à l'extrémité PE. L'extrémité PE communique avec les entités P et les extrémités PE et établit une connexion le long du trajet spécifié par le contrôleur PCC. Le contrôleur PCC agit comme un point de décision de politique, tandis que l'extrémité PE agit comme un point d'application de la politique, comme indiqué au § 7.3. L'extrémité PE peut identifier le réseau à partir duquel la demande de connexion est émise, en utilisant le mécanisme mentionné au § 8.2.2.

Lorsque les informations sur les membres sont optionnellement échangées entre le client et le réseau, le contrôleur PCC communique avec les extrémités PE qui à leur tour communiquent avec les extrémités CE pour échanger les informations sur les membres. De plus, lorsque l'information d'acheminement est optionnellement échangée entre le client et le réseau, le contrôleur PCC et les extrémités PE disposent d'un Plan C exclusif leur permettant de classer l'information de topologie par réseau VPN. Si les entités P disposent également d'un Plan C exclusif, le Plan C exclusif du contrôleur PCC communique avec le Plan C exclusif des extrémités PE, et le Plan C exclusif des extrémités PE communique avec les extrémités CE pour ce qui est de l'information de ressource par réseau VPN du réseau du fournisseur. Egalement, le Plan C exclusif des extrémités PE peut communiquer avec les extrémités CE pour échanger l'information d'acheminement du domaine client et l'information de connectivité.

Si les entités P disposent d'un Plan C partagé, le contrôleur PCC classe l'information de topologie du réseau par réseau VPN, en transférant l'information de topologie du réseau depuis une instance partagée vers des instances exclusives en utilisant des mécanismes analogues mentionnés pour le Plan C exclusif de l'extrémité PE, au § 10.1. Le Plan C exclusif du contrôleur PCC communique avec le Plan C exclusif des extrémités PE, et le Plan C exclusif des extrémités PE communique avec les extrémités CE.

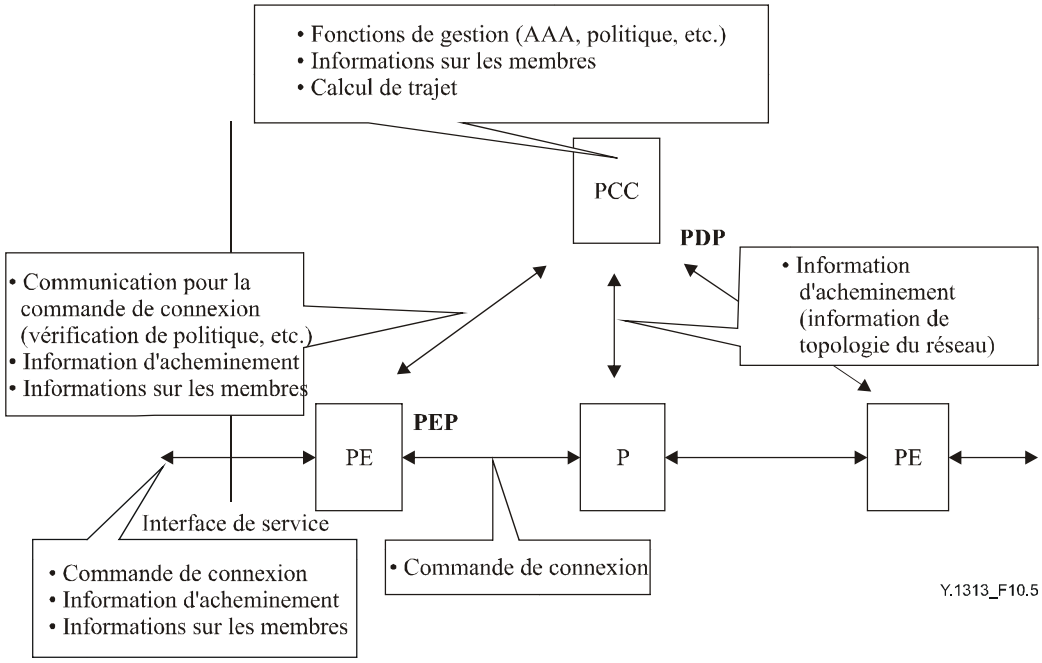

Figure 10-5/Y.1313 – Communication décentralisée avec le client

2) Communication centralisée avec le client

Dans ce modèle, le contrôleur PCC communique avec des entités clients, tels les contrôleurs CCC. Le contrôleur PCC reçoit une demande de connexion émanant d'un client et vérifie s'il y a une autorisation de connexion en procédant à une vérification de restriction de connectivité ainsi qu'à une vérification du niveau de service. Le contrôleur PCC calcule ensuite un trajet et communique avec une extrémité PE. L'extrémité PE communique à son tour avec les entités P et les extrémités PE et établit une connexion le long du trajet spécifié par le contrôleur PCC. Le contrôleur PCC agit comme point PDP et PEP, comme indiqué au § 7.3. Le contrôleur PCC doit identifier le réseau VPN d'où émane la demande de connexion.

Le contrôleur PCC peut optionnellement communiquer avec les entités clients pour échanger les informations sur les membres. Le contrôleur PCC peut aussi optionnellement disposer d'un Plan C exclusif pour classer l'information de topologie par réseau VPN. Le contrôleur PCC peut communiquer avec les entités clients pour donner, par réseau VPN, l'information sur les ressources du réseau du fournisseur. Le contrôleur PCC peut en outre communiquer avec des entités clients pour échanger l'information d'acheminement du domaine client et l'information de connectivité.

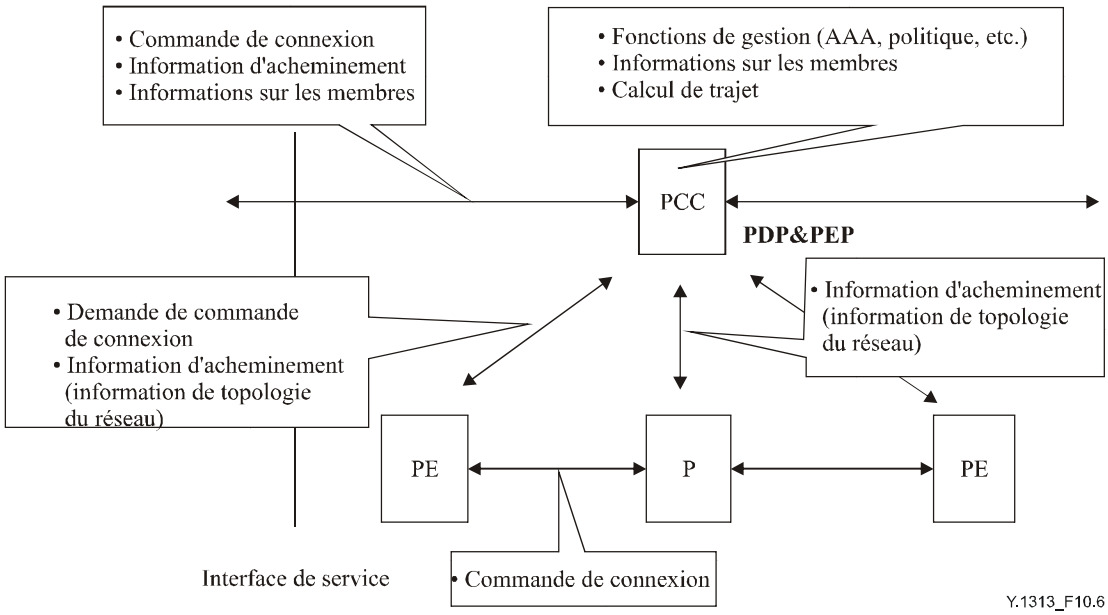

Figure 10-6/Y.1313 – Communication centralisée avec le client

10.3 Architecture centralisée de réseau du fournisseur

Dans ce modèle, le contrôleur PCC communique avec les entités clients, qui sont en général des contrôleurs CCC. En outre, le contrôleur PCC communique avec les extrémités PE et les entités P pour obtenir l'information de topologie du réseau tout comme pour demander la commande de connexion.

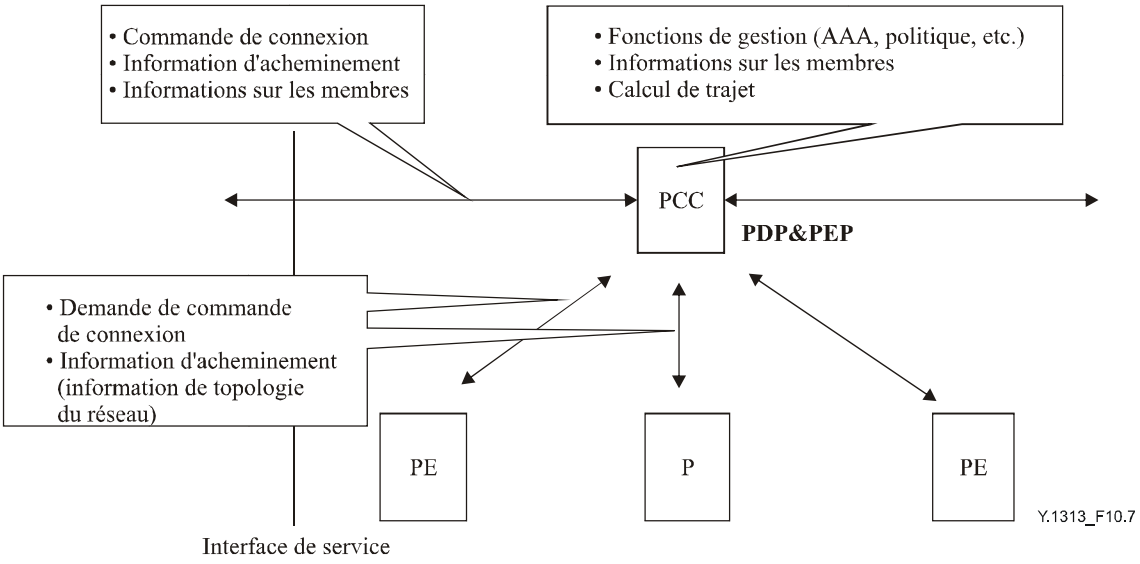

Figure 10-7/Y.1313 – Architecture centralisée de réseau du fournisseur

11 Exemples d'implémentation des architectures fonctionnelles

11.1 Aperçu général

Les mécanismes existants qui peuvent être appliqués aux réseaux VPN L1 peuvent varier en fonction des types d'architectures de réseaux VPN L1. En général, toutefois, on peut retenir les hypothèses suivantes:

- *Tenue à jour des informations sur les membres*

On peut utiliser les mécanismes applicables aux réseaux VPN L2 et L3. Par exemple, on peut utiliser des mécanismes fondés sur l'acheminement (par exemple sur le BGP [IETF RFC 1771]) ou sur les annuaires. Des mécanismes analogues peuvent être utilisés pour l'exploration des réseaux (par exemple, l'exploration des extrémités PE distantes, l'exploration des contrôleurs PCC).

Des mécanismes permettant de répartir les informations sur les membres à l'intérieur du réseau du fournisseur peuvent être différents des mécanismes permettant de communiquer avec les entités clients.

- *Tenue à jour de l'information d'acheminement et calcul de trajet*

Les protocoles d'états de liaison tel l'OSPF peuvent être appliqués (par exemple [IETF RFC 2328]) avec des extensions appropriées. Pour ventiler l'information de topologie par réseau VPN, on peut utiliser des mécanismes fondés sur des routeurs virtuels ou l'extension des protocoles d'acheminement permettant d'acheminer l'identificateur VPN ID spécifiant le réseau VPN auquel l'information appartient.

Les mécanismes permettant de distribuer l'information de topologie à l'intérieur du réseau du fournisseur peuvent être différents des mécanismes permettant de communiquer avec des entités clients.

L'information statique, telle que l'information contractuelle sur les ressources attribuées à titre exclusif, peut être obtenue via l'interface CNM.

A noter que le calcul de trajet est un processus de décision locale et, en général, ne fait intervenir de protocole.

- *Commande de connexion*

Des protocoles de signalisation du plan de commande optique (par exemple [IETF RFC 3473], [IETF RFC 3472], [IETF RFC 3474], [IETF RFC 3475], [IETF RFC 3476], [UIT-T G.7713.1], [UIT-T G.7713.2], [UIT-T G.7713.3], [OIF UNI 1.0], [OIF Signaling E-NNI 1.0]) peuvent être appliqués.

- *Gestion*

Tout comme pour les informations relatives à la gestion, telles les informations de performance et les informations d'enregistrement (facturation), l'interface CNM peut être utilisée en passant par des mécanismes tels le CORBA, les services Web et le FTP.

Pour la communication entre le contrôleur PCC et le PE/P, on peut utiliser les protocoles TMF814, SNMP, XML et TL-1. De plus, dans l'architecture hybride de fournisseur de réseau, on exige la présence de mécanismes permettant la communication entre le contrôleur PCC et l'extrémité PE, et on peut utiliser des protocoles de type politique tel le COPS [IETF RFC 2748].

Une autre classe de mécanismes englobe les aspects gestion de la configuration du réseau (mécanismes d'autodécouverte) et gestion des anomalies/de la performance (tels des mécanismes OAM spécifiques des technologies utilisées).

- *Support L1*

Un support L1 peut prendre en charge les services L1 de base, décrits dans la Rec. UIT-T Y.1312. Parmi les technologies support L1 concernées, il y a des technologies SONET/SDH, OTN, et les lignes privées Ethernet (EPL).

Les paragraphes qui suivent décrivent les éventuels mappages détaillés entre les mécanismes existants et les fonctions VPN L1, dans différents exemples d'architecture mentionnés au § 10. Comme indiqué plus loin, ces mécanismes sont donnés uniquement à titre d'exemples et comme solution envisageable, leur applicabilité réelle ne relevant pas du domaine d'application de la présente Recommandation.

L'Appendice I donne une liste d'exemples d'implémentation de ces mécanismes.

11.2 Architecture décentralisée de réseau du fournisseur

Le § 10.1 décrit trois modèles d'architecture décentralisée de réseau du fournisseur à savoir le Plan C exclusif, le Plan C attribué à titre exclusif à l'extrémité PE et le Plan C partagé. Les paragraphes qui suivent décrivent comment les mécanismes existants peuvent être appliqués à chaque modèle.

1) Plan C exclusif

Dans ce modèle, les ressources du Plan U sont généralement attribuées à titre exclusif.

On peut utiliser des routeurs virtuels pour répartir le Plan C par réseau VPN. En outre, la signalisation et l'acheminement dans le plan de commande optique peuvent être utilisés pour la communication à l'intérieur du Plan C exclusif. Certains exemples de mécanismes/de solutions protocolaires sont donnés dans le Tableau 11-1 et la Figure 11-1 ci-dessous.

Tableau 11-1/Y.1313 – Plan C exclusif

		CE-PE		**A l'intérieur du réseau du fournisseur**
		Pas d'échange d'information d'acheminement	**Avec échange d'information d'acheminement**	
Tenue à jour des informations sur les membres		BGP, mécanismes fondés sur les annuaires	BGP, mécanismes fondés sur les annuaires, mécanismes pour la tenue à jour de l'information d'acheminement	BGP, mécanismes fondés sur les annuaires, mécanismes pour la tenue à jour de l'information d'acheminement
Tenue à jour de l'information d'achemi-nement	Information d'acheminement du domaine client	Néant	Acheminement dans le plan de commande optique pour I-NNI, E-NNI	Acheminement dans le plan de commande optique par VPN
	Information de connectivité			
	Information de topologie du réseau			
Commande de connexion		Signalisation dans le plan de commande optique pour l'UNI	Signalisation dans le plan de commande optique pour I-NNI, E-NNI	Signalisation dans le plan de commande optique par VPN
Aspects gestion		Mécanismes d'auto-exploration, mécanismes OAM	Mécanismes d'auto-exploration, mécanismes OAM	Mécanismes d'auto-exploration, mécanismes OAM

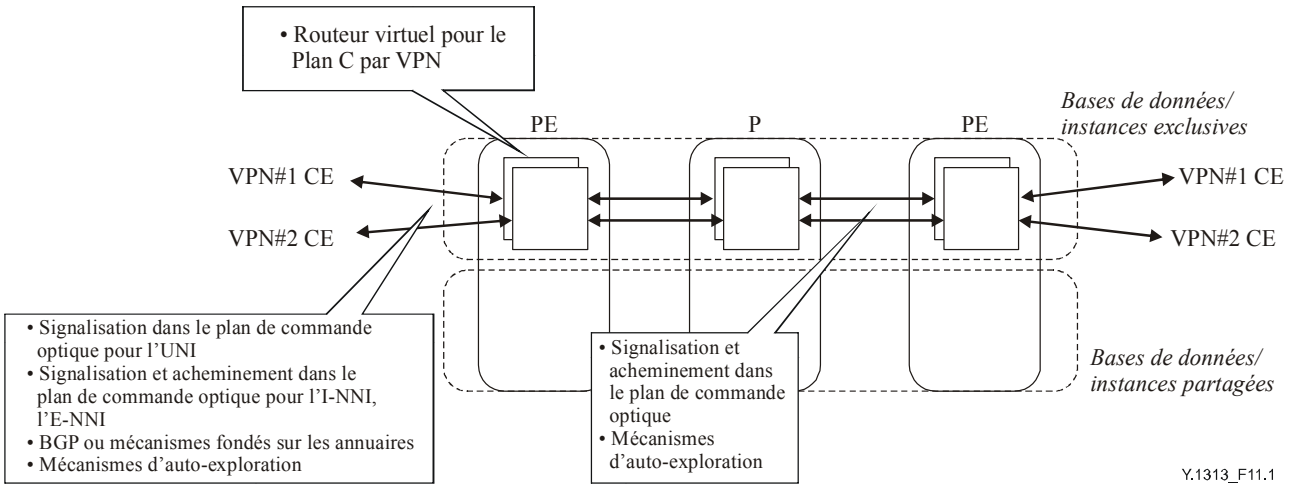

Figure 11-1/Y.1313 – Plan C exclusif

2) Plan C attribué à titre exclusif aux extrémités PE

Dans ce modèle, les ressources du Plan U sont attribuées à titre exclusif ou partagées.

A l'interface CE-PE, différents mécanismes peuvent être appliqués selon que l'information d'acheminement est échangée entre le client et le réseau ou non. Si l'information d'acheminement n'est pas échangée, la signalisation dans le plan de commande optique pour l'interface UNI peut être utilisée pour la commande de connexion. En outre, le protocole BGP ou des mécanismes fondés sur l'annuaire peuvent être appliqués pour la tenue à jour des informations sur les membres. Les informations sur les membres peuvent également être insérées dans l'information d'acheminement. Par ailleurs, si l'information d'acheminement est échangée, la signalisation et l'acheminement dans le plan de commande optique peuvent être utilisés pour la tenue à jour de l'information d'acheminement et la commande de connexion. Au niveau de l'extrémité PE, des routeurs virtuels peuvent être utilisés pour répartir l'information d'acheminement par réseau VPN. De plus, les mécanismes permettant de résumer les données de topologie interdomaines peuvent être appliqués lorsqu'on fournit de l'information résumée de topologie au client. Entre les extrémités PE, des mécanismes d'établissement de tunnels tels les mécanismes de tunnel IP, peuvent être appliqués pour établir un tunnel entre les extrémités PE sur le Plan C. De plus, des mécanismes d'auto-exploration utilisant le protocole BGP fondés sur les annuaires peuvent être utilisés pour explorer les extrémités PE distantes.

Dans le réseau du fournisseur, l'acheminement et la signalisation du plan de commande optique peuvent être utilisés pour la tenue à jour de l'information d'acheminement et la commande de connexion. A noter que pour ventiler l'information de topologie du réseau par VPN au niveau de l'extrémité PE, par exemple, une information d'acheminement associée à l'identificateur VPN ID peut être échangée dans le réseau du fournisseur, spécifiant le réseau VPN auquel chaque liaison appartient. Des exemples de mécanismes ou de solutions protocolaires sont donnés dans le Tableau 11-2 et la Figure 11-2 ci-dessous.

Tableau 11-2/Y.1313 – Plan C attribué à titre exclusif aux extrémités PE

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">CE-PE</th><th rowspan="2">A l'intérieur du réseau du fournisseur</th></tr>
<tr><th>Pas d'échange d'information d'acheminement</th><th>Avec échange d'information d'acheminement</th></tr>
<tr><td colspan="2">Tenue à jour des informations sur les membres</td><td>BGP, mécanismes fondés sur les annuaires</td><td>BGP, mécanismes fondés sur les annuaires, mécanismes de tenue à jour de l'information d'acheminement</td><td>BGP, mécanismes fondés sur les annuaires, mécanismes de tenue à jour de l'information d'acheminement</td></tr>
<tr><td rowspan="3">Tenue à jour de l'information d'achemi-nement</td><td>Information d'acheminement du domaine client</td><td rowspan="3">Néant</td><td rowspan="3">Acheminement dans le plan de commande optique pour l'I-NNI, l'E-NNI</td><td>Acheminement dans le plan de commande optique par VPN sur le tunnel du Plan C entre PE</td></tr>
<tr><td>Information de connectivité</td><td></td></tr>
<tr><td>Information de topologie du réseau</td><td>Acheminement commun dans le plan de commande optique</td></tr>
<tr><td colspan="2">Commande de connexion</td><td>Signalisation dans le plan de commande optique pour l'UNI</td><td>Signalisation dans le plan de commande optique pour l'I-NNI, l'E-NNI</td><td>Signalisation commune dans le plan de commande optique</td></tr>
<tr><td colspan="2">Aspects de gestion</td><td>Mécanismes d'auto-exploration, mécanismes OAM</td><td>Mécanismes d'auto-exploration, mécanismes OAM</td><td>Mécanismes d'auto-exploration, mécanismes OAM</td></tr>
</table>

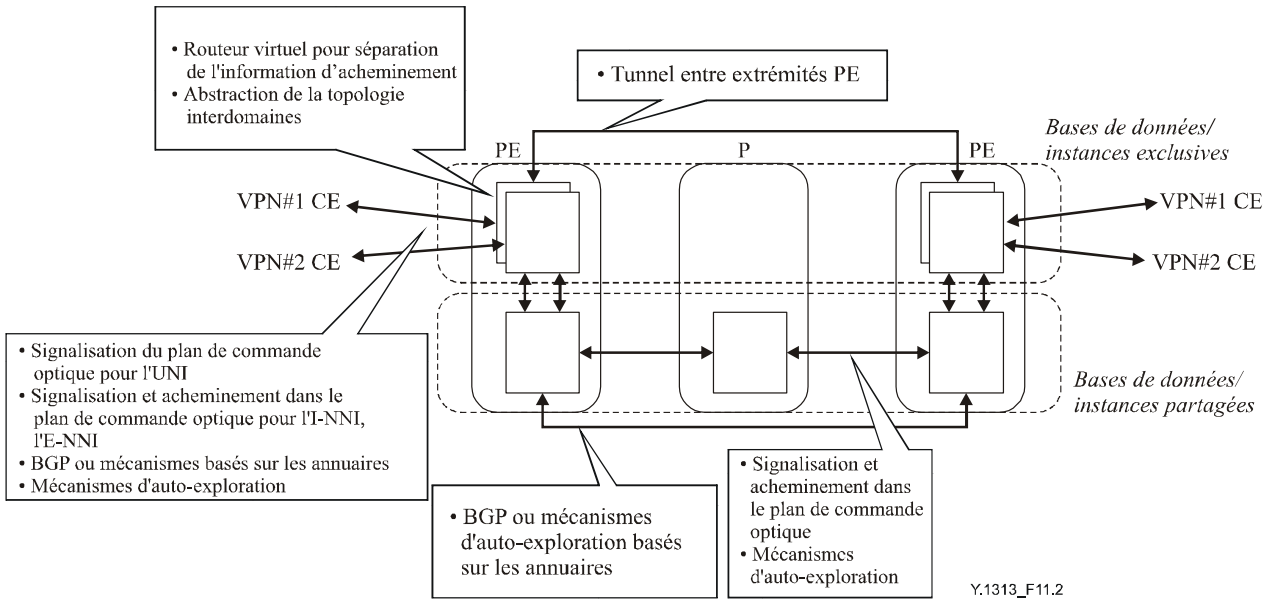

Figure 11-2/Y.1313 – Plan C attribué à titre exclusif aux extrémités PE

3) Plan C partagé

Dans ce modèle, les ressources du Plan U sont attribuées à titre exclusif ou partagées.

Etant donné qu'il n'y a pas d'échange d'informations d'acheminement entre le client et le réseau, la signalisation dans le plan de commande optique pour l'UNI peut être utilisée entre les extrémités CE (ou entité client) et l'extrémité PE. De plus, le protocole BGP et les mécanismes basés sur les annuaires peuvent être appliqués pour la tenue à jour des informations sur les membres. Les informations sur les membres peuvent être également insérées dans l'information d'acheminement. L'auto-exploration peut être obtenue au moyen de divers mécanismes.

Dans le réseau du fournisseur, la signalisation et l'acheminement dans le plan de commande optique peuvent être appliqués pour la tenue à jour de l'information d'acheminement et la commande de connexion. De plus, le protocole BGP ou les mécanismes d'auto-exploration et d'échange d'informations sur les membres fondés sur les annuaires peuvent être utilisés entre les extrémités PE. Certains exemples de mécanismes/de solutions protocolaires sont donnés dans le Tableau 11-3 et la Figure 11-3 ci-dessous.

Tableau 11-3/Y.1313 – Plan C partagé

		CE-PE		A l'intérieur du réseau du fournisseur
		Pas d'échange d'information d'acheminement	**Avec échange d'information d'acheminement**	
Tenue à jour des informations sur les membres		BGP, mécanismes fondés sur les annuaires	–	BGP, mécanismes fondés sur les annuaires, mécanismes de tenue à jour de l'information d'acheminement
Tenue à jour de l'information d'acheminement	Information d'acheminement du domaine client	Néant	–	–
	Information de connectivité			–
	Information de topologie du réseau			Acheminement commun dans le plan de commande optique
Commande de connexion		Signalisation dans le plan de commande optique pour l'UNI	–	Signalisation commune dans le plan de commande optique
Aspects de gestion		Mécanismes d'auto-exploration, mécanismes OAM	–	Mécanismes d'auto-exploration, mécanismes OAM

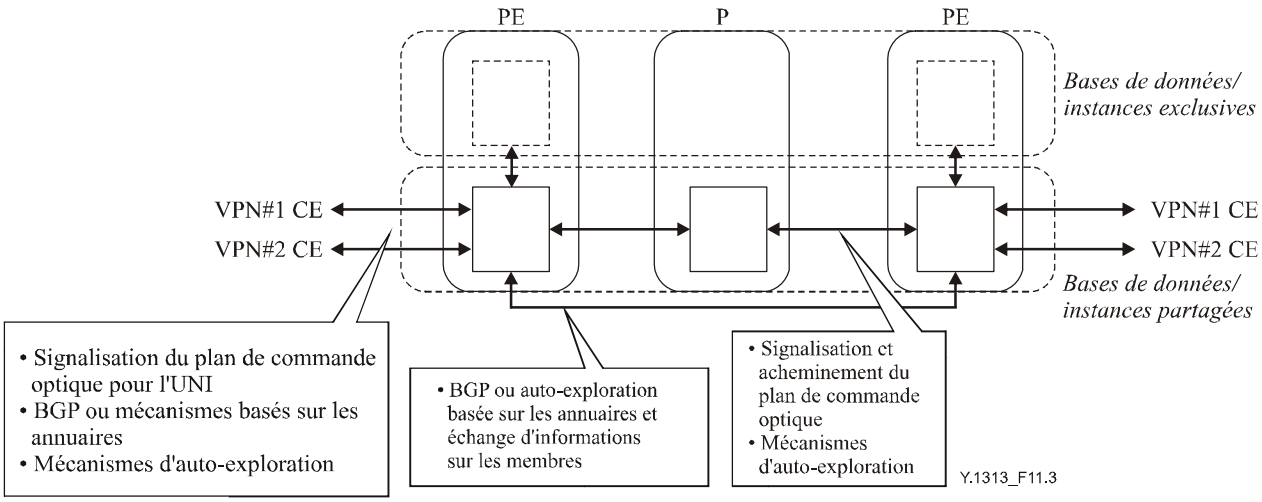

Figure 11-3/Y.1313 – Plan C partagé

11.3 Architecture hybride de fournisseur de réseau

Le § 10.2 contient un exemple d'architecture hybride de fournisseur de réseau, dans lequel les fonctions de service propres au VPN L1, telles la tenue à jour des informations sur les membres ainsi que les fonctions de gestion, sont centralisées, tandis que les fonctions communes permettant d'établir des connexions L1, telle la commande de connexion, sont décentralisées. Dans ce type d'architecture, deux modèles de communication avec le client peuvent être pris en considération. L'un est un modèle à communication décentralisée et l'autre à communication centralisée. Même s'il y a de nombreuses fonctions communes dans les deux modèles, les fonctions requises diffèrent entre les modèles dans certains domaines. En tant que telles, les différences entre les deux modèles portent sur la façon dont existent les mécanismes qui peuvent être appliqués aux fonctions VPN L1.

1) Communication décentralisée avec le client

Dans ce modèle, au niveau de l'interface CE (ou entité client)-PE, différents mécanismes peuvent être appliqués selon que l'information d'acheminement est échangée entre le client et le réseau ou non. Si l'information d'acheminement n'est pas échangée, la signalisation dans le plan de commande optique pour l'interface UNI peut être utilisée pour la commande de connexion. De plus, le protocole BGP ou des mécanismes fondés sur les annuaires peuvent être appliqués pour la tenue à jour des informations sur les membres. L'auto-exploration peut être obtenue par divers mécanismes. Par ailleurs, si l'information d'acheminement est échangée, l'acheminement et la signalisation dans le plan de commande optique peuvent être utilisés pour la tenue à jour de l'information d'acheminement et la commande de connexion.

Dans le réseau du fournisseur, la signalisation dans le plan de commande optique peut être utilisée pour la commande de connexion. Les protocoles sur les politiques, tels le COPS ou le TMF814, peuvent être appliqués pour la communication destinée à la commande de connexion entre le contrôleur PCC et l'extrémité PE. Le contrôleur PCC participe à l'acheminement dans le plan de commande optique et obtient l'information concernant la topologie du réseau du fournisseur. Ou bien il recueille l'information sur la topologie du réseau du fournisseur via les mécanismes fondés sur la gestion, tel le TMF814. Lorsque l'information d'acheminement a été échangée entre le client et le réseau, des routeurs virtuels peuvent être utilisés pour ventiler l'information d'acheminement par réseau VPN au niveau du contrôleur PCC et aussi au niveau de l'extrémité PE. Lorsque l'information de topologie fournie au client est résumée, on peut résumer la topologie interdomaines appliquée au contrôleur PCC. L'information de topologie par réseau VPN obtenue au contrôleur PCC est échangée avec des routeurs virtuels, et ces routeurs virtuels communiquent avec les extrémités CE (ou les entités clients) pour échanger l'information d'acheminement. Voir la Figure 11-4.

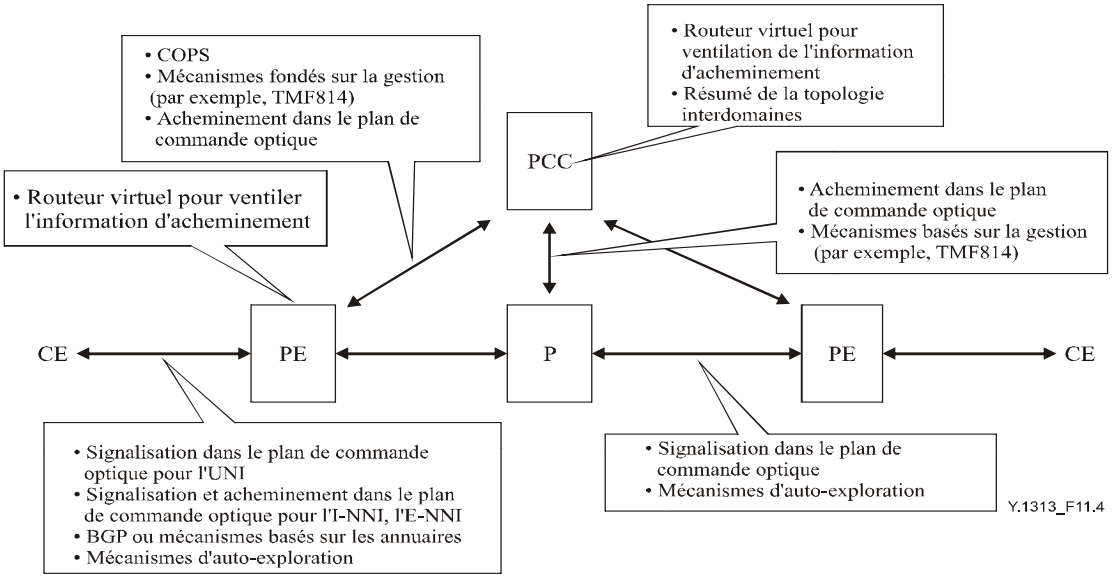

Figure 11-4/Y.1313 – Communication décentralisée avec le client

2) Communication centralisée avec le client

Dans ce modèle, à l'interface CCC (ou entité client)-PCC, différents mécanismes peuvent être appliqués selon que l'information d'acheminement est échangée entre le client et le réseau ou non, et selon les types d'interface. Si l'information d'acheminement n'est pas échangée, la signalisation dans le plan de commande optique pour l'interface UNI peut être utilisée pour la commande de connexion. De plus, le protocole BGP ou des mécanismes basés sur les annuaires peuvent être appliqués pour la tenue à jour des informations sur les membres. Par ailleurs, s'il y a échange des informations d'acheminement, l'acheminement et la signalisation dans le plan de commande optique peuvent être utilisés pour la tenue à jour de l'information d'acheminement et la commande de connexion. Si la gestion CNM ou le type de gestion de l'interface est utilisé entre le contrôleur CCC (ou l'entité client) et le contrôleur PCC, des mécanismes basés sur la gestion sont utilisés pour l'échange des informations entre le contrôleur CCC (ou l'entité client) et le contrôleur PCC.

Dans le réseau du fournisseur, la signalisation dans le plan de commande optique peut être utilisée pour la commande de connexion. Des mécanismes de connexion permanente reconfigurable (SPC, *soft permanent connection*) peuvent être utilisés entre le contrôleur PCC et l'extrémité PE pour déclencher l'établissement d'une connexion au niveau de l'extrémité PE. Le contrôleur PCC participe à l'acheminement et obtient l'information de topologie de la part du fournisseur de réseau. Ou bien, il recueille l'information de topologie du réseau du fournisseur via des mécanismes basés sur la gestion, tel le TMF814. Lorsque l'information d'acheminement est échangée entre le client et le réseau, des routeurs virtuels peuvent être utilisés pour ventiler l'information d'acheminement par réseau VPN au niveau du contrôleur PCC. Lorsque l'information de topologie fournie au client est résumée, la topologie interdomaines peut être résumée au niveau du contrôleur PCC.

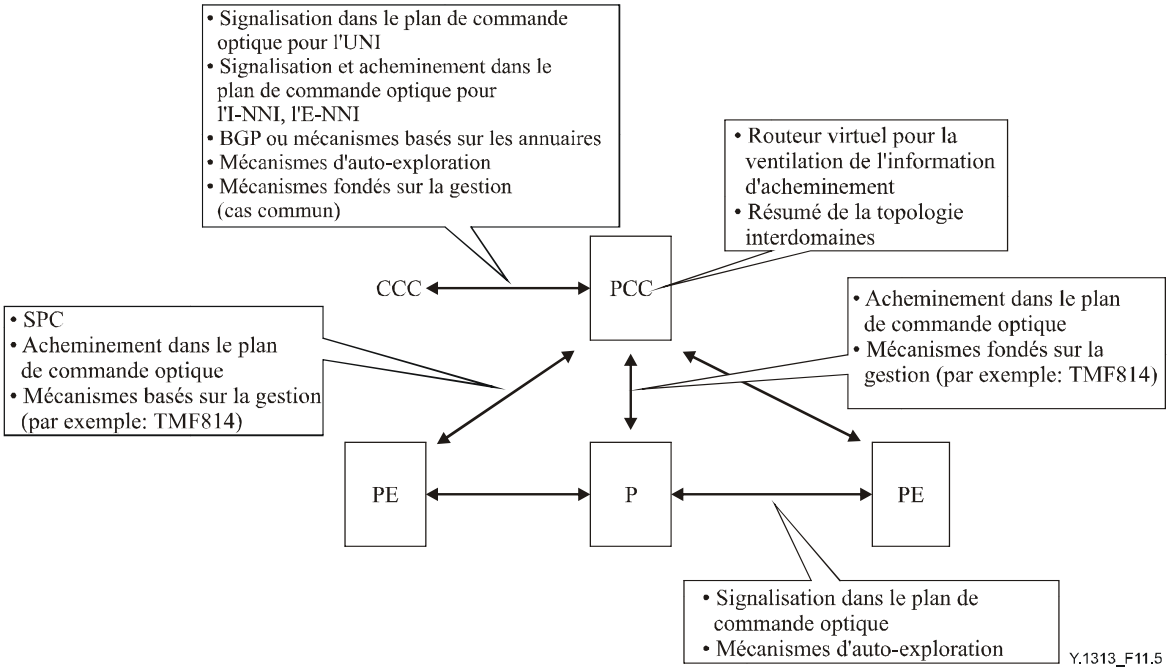

Figure 11-5/Y.1313 – Communication centralisée avec le client

11.4 Architecture centralisée de réseau du fournisseur

Dans le cas d'une architecture centralisée de réseau du fournisseur, en général, le contrôleur PCC communique avec le contrôleur CCC au moyen de mécanismes basés sur la gestion. De plus le contrôleur PCC communique avec les extrémités PE et les entités P au moyen de mécanismes fondés sur la gestion. Il n'y a pas de signalisation décentralisée parmi les extrémités PE et les entités P.

12 Aspects sécurité

Il n'y a pas d'exigences en matière de sécurité autres que celles indiquées dans la Rec. UIT-T Y.1312.

Annexe A

Description détaillée des extrémités CE et PE

A.1 Architecture d'extrémités CE participant à plusieurs réseaux VPN de couche 1 (structures extraites des Recommandations UIT-T G.805 et G.8080/Y.1304)

Une extrémité CE est un groupement administratif de conteneurs de groupes d'accès (AGC, *access group containers*) (voir Amendement 1 à la Rec. UIT-T G.8080/Y.1304) et d'applications VPN de couche 1. Un conteneur AGC fournit un lieu pour les services à une application VPN de couche 1. Une application VPN de couche 1 est constituée d'un ou plusieurs utilisateurs de connexion (CU, *connection user*) et d'agents d'appel client (CCA, *customer call agents*) (noter que le terme CCA provenant de la Rec. UIT-T Y.1312 et le terme demandeur de connexion *(connection requestor*) de l'Amendement 1 de la Rec. UIT-T G.8080/Y.1304 désignent la même entité). Il n'y a qu'un seul conteneur AGC par application VPN de couche 1 par extrémité CE.

A partir du point de vue du Plan U, la Figure A.1 illustre la relation directe qui existe entre les utilisateurs CU de réseau VPN de couche 1 et les AG. A noter que AG_2 appartient à la fois à l'AGC_A et à l'AGC_B pour les réseaux VPN de Couches A et B (il s'agit d'une extension de l'Amendement 1 de la Rec. UIT-T G.8080/Y.1304). Cela est nécessaire pour permettre le partage du Plan U entre des réseaux VPN de couche 1.

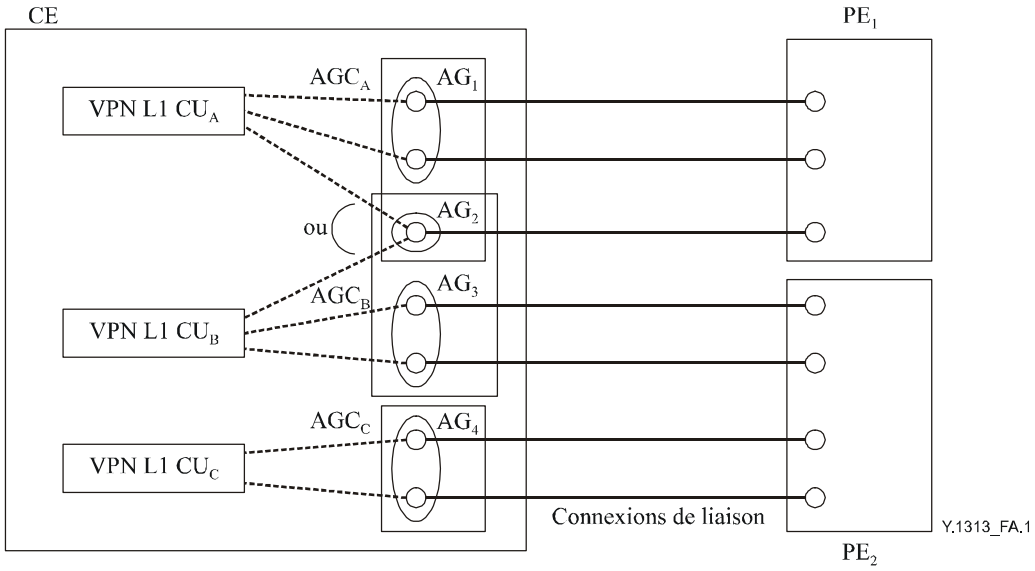

Figure A.1/Y.1313 – Exemple d'architecture du Plan U pour les extrémités CE et PE

Du point de vue du Plan C, la Figure A.2 illustre la relation qui existe entre les agents CCA de réseau VPN de couche 1 et les liaisons SNPP contenues dans les conteneurs AGC.

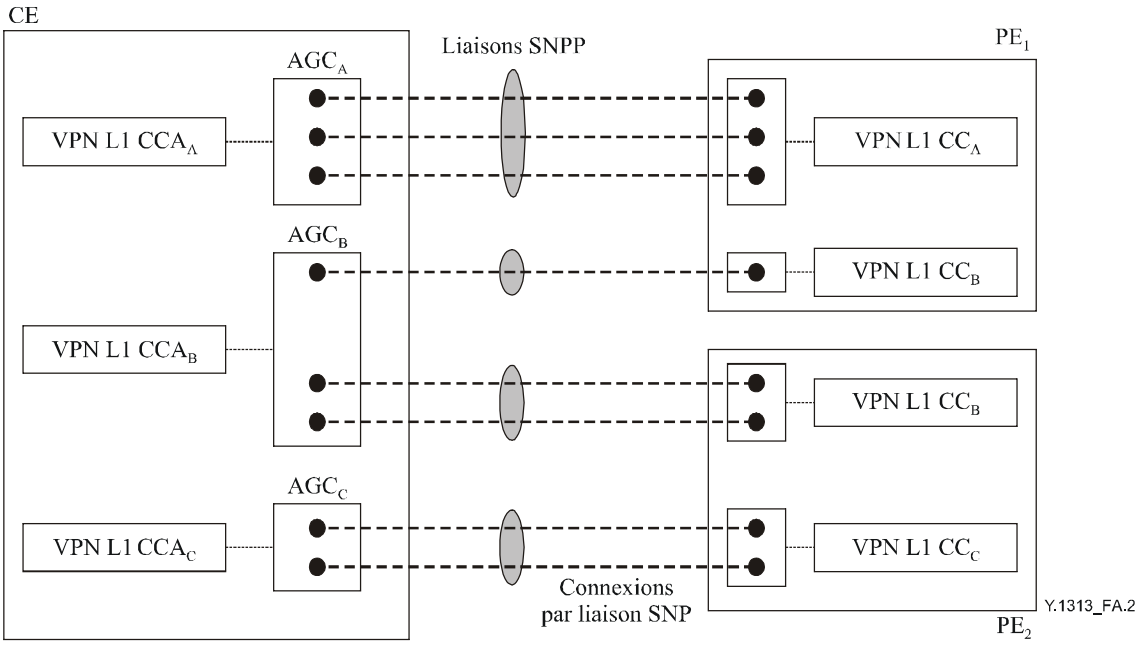

Figure A.2/Y.1313 – Exemple d'architecture du Plan C pour les extrémités CE et PE

A.2 Architecture d'une extrémité PE participant à plusieurs réseaux VPN de couche 1 (structures émanant des Recommandations UIT-T G.805 et G.8080/Y.1304)

Dans la mesure où elle se rapporte à l'extrémité CE, l'extrémité PE est un groupement administratif de connexions de liaisons et de liaisons SNPP. Le groupage est soumis aux deux contraintes suivantes:

1) des connexions par liaison associées au même AG sur une extrémité CE doivent appartenir à la même extrémité PE (contrainte du Plan U);

2) la fermeture de toutes les liaisons SNPP, qui contiennent des connexions de liaisons SNP qui sont autorisées à être liées aux mêmes connexions de liaisons par configuration, doit relever de la même extrémité PE (contrainte du Plan C).

De plus, on suppose que l'extrémité PE a une connaissance explicite des appartenances des liaisons SNPP avec les réseaux VPN de couche 1. Cela a pour conséquence que l'extrémité PE dispose d'un contrôleur de connexion (CC) par réseau VPN de couche 1. L'architecture de l'extrémité PE et la façon dont elle est liée à l'extrémité CE sont illustrées dans les Figures A.1 et A.2. Dans cet exemple, le réseau VPN L1 B sur l'extrémité CE est rattaché à la fois aux extrémités PE_1 et PE_2. Dans cet exemple, on suppose aussi que le Plan C est attribué à titre exclusif étant donné qu'il y a un contrôleur de connexion par réseau VPN de couche 1 par extrémité PE. D'autres fonctions et d'autres propriétés de l'extrémité PE sont volontairement non spécifiées.

A.3 Architecture des extrémités CE et PE en rapport avec les systèmes de gestion

Dans l'architecture des extrémités CE et PE décrite dans le paragraphe précédent, on suppose que l'architecture de commande de réseau VPN de couche 1 est décentralisée. Toutefois, l'architecture de commande de réseau VPN de couche 1 peut aussi être centralisée. Cela impose la présence d'entités de gestion, à savoir: le système de gestion client (CMS, *customer management system*) et le système de gestion du fournisseur (PMS, *provider management system*). A noter que les fonctions des contrôleurs CCC et PCC sont instanciées dans les systèmes CMS et PMS respectivement. De plus, l'architecture des extrémités CE et PE doit être prolongée par des interfaces de gestion. En particulier, il peut y avoir une interface gestion du réseau par le client (CNM, *customer network management*) entre les entités clients et le système de gestion du fournisseur. En outre, il peut également y avoir une interface de contrôle de délégation entre le système de gestion client et l'extrémité PE. Finalement, il existe des interfaces de gestion internes au client et au fournisseur. L'ensemble général d'interface de commande est illustré à la Figure A.3.

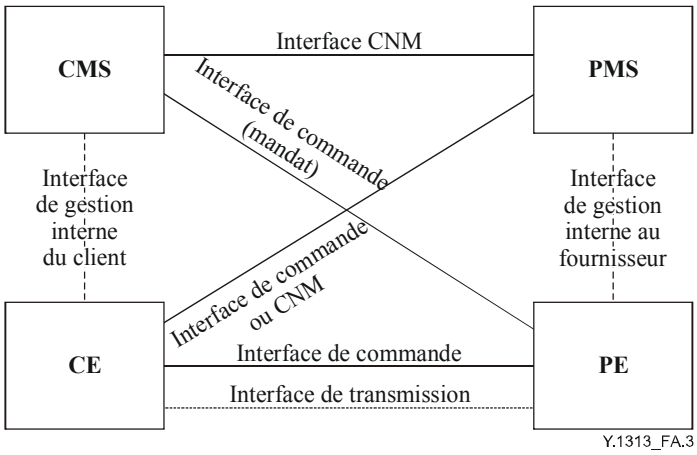

Figure A.3/Y.1313 – Interfaces globales CE-PE, incluant l'aspect gestion

Appendice I

Exemple d'implémentation de mécanismes existants pour les réseaux VPN de couche 1

Des exemples d'implémentation de mécanismes existants qui peuvent être appliqués aux fonctions des réseaux VPN de couche 1 sont donnés ci-dessous. A noter que les mécanismes décrits dans le présent appendice ne constituent que des exemples. La présente Recommandation n'exclut pas d'autres mécanismes qui pourraient être appliqués pour la prise en charge des services VPN de couche 1. A noter également qu'il pourrait s'avérer nécessaire d'étendre les mécanismes décrits dans le présent appendice afin qu'ils puissent prendre en charge les services VPN de couche 1.

Tableau I.1/Y.1313 – Exemple de mécanismes existants pour les réseaux VPN de couche 1

Tenue à jour des informations sur les membres		
	Exemple de mécanismes basés sur l'acheminement	[IETF RFC 2547 *bis*], [IETF GVPN]
Tenue à jour de l'information d'acheminement et calcul de trajet		
	Exemple de protocole d'acheminement du plan de commande optique	[IETF GMPLS OSPF], [OIF Routing E-NNI 1.0]
	Exemple de mécanismes basés sur des routeurs virtuels	[IETF VR], [IETF GVPN]
Commande de connexion		
	Exemple de signalisation du plan de commande optique pour l'UNI	[IETF GMPLS Overlay], [OIF UNI 1.0], [UIT-T G.7713.2], [UIT-T G.7713.3], [IETF RFC 3474], [IETF RFC 3475], [IETF RFC 3476]
	Exemple de signalisation du plan de commande optique pour l'I-NNI, l'E-NNI	[IETF RFC 3473], [IETF RFC 3472], [UIT-T G.7713.1], [UIT-T G.7713.2], [UIT-T G.7713.3], [IETF RFC 3474], [IETF RFC 3475], [OIF Signaling E-NNI 1.0]
Gestion		
	Exemple d'interface CNM	CORBA, services Web, FTP
	Exemple de communication entre le PCC et le PE/P	TMF814, SNMP, XML, TL-1
	Exemple de protocoles de politique	[IETF RFC 2748]
	Exemple de mécanismes d'auto-exploration	[IETF LMP], [OIF UNI 1.0], [UIT-T G.7714.1]

BIBLIOGRAPHIE

[IETF RFC 2547 *bis*] ROSEN (E.), REKHTER (Y.): BGP/MPLS IP VPNs, (draft-ietf-l3vpn-rfc2547bis-01.txt), *work in progress in IETF*.

[IETF GVPN] OULD-BRAHIM (H.), REKHTER (Y.): GVPN Services: Generalized VPN Services using BGP and GMPLS Toolkit, (draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-04.txt), *work in progress in IETF*.

[IETF GMPLS OSPF] KOMPELLA (K.), REKHTER (Y.): OSPF Extensions in Support of Generalized Multi-Protocol Label Switching, (draft-ietf-ccamp-ospf-gmpls-extensions-12.txt), *work in progress in IETF*.

[OIF Routing E-NNI 1.0] ONG (L), *et al*.: Draft OIF Specification for Intra-Carrier E-NNI Routing using OSPF (*oif2003.259*).

[IETF VR] KNIGHT (P.), OULD-BRAHIM (H.): Network based IP VPN Architecture using Virtual Routers, (draft-ietf-l3vpn-vpn-vr-01.txt), *work in progress in IETF*.

[IETF GMPLS Overlay] SWALLOW (G.), *et al*.: GMPLS UNI: RSVP-TE Support for the Overlay Model, (draft-ietf-ccamp-gmpls-overlay-04.txt), *work in progress in IETF*.

[IETF LMP] LANG (J.): Link Management Protocol (LMP), (draft-ietf-ccamp-lmp-10.txt), *work in progress in IETF*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005